DOCUMENT RESUME

ED 212 293 IR 010 002

TITLE	Data Processing Technician 1 & C. Revised 1981.
INSTITUTION	Naval Education and Training Program Development Center, Pensacola, Fla.
SPONS AGENCY	Chief of Naval Education and Training Support, Pensacola, Fla.
REPORT NO	NAVEDTRA-10265-D
PUB DATE	81
NOTE	298p.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402 (Stock No. 0502-LP-051-3262)
EDRS PRICE	MF01/PC12 Plus Postage.
DESCRIPTORS	*Data Processing; *Data Processing Occupations; Independent Study; *Management Development; Military Personnel; *Technical Education
IDENTIFIERS	*Naval Training

ABSTRACT

This Rate Training Manual and Nonresident Career Course (RTM/NRCC) is intended to serve as an aid for Navy personnel who are seeking to acquire the management and operational skills required of candidates for advancement to the rate of Data Processing Technician First Class or Data Processing Technician Chief. Designed for individual study, the RTM provides subject matter that relates directly to the occupational qualifications for data processing. The NRCC that accompanies this RTM provides the necessary requirements for completing the RTM. (Author/LLS)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

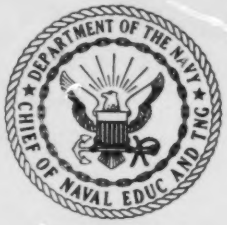
U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION
CENTER (ERIC)
☒ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

ED212293

Naval Education And Training Program Development Center

DATA PROCESSING TECHNICIAN 1 & C

NAVEDTRA 10265-D



1981 Edition Prepared by
DPCS Lawrence G. Dunlap

IR 010002

PREFACE

This Rate Training Manual and Nonresident Career Course (RTM/NRCC) is intended to serve as an aid for personnel who are seeking to acquire the management and operational skills required of candidates for advancement to the rate of Data Processing Technician First Class or Data Processing Technician Chief.

Designed for individual study, the RTM provides subject matter that relates directly to the occupational qualifications for DP. It is recommended that personnel studying this training package should have completed the Data Processing Technician 3 & 2 course. The NRCC that accompanies this RTM provides the necessary requirements for completing the RTM. Before starting your study, browse the entire RTM/NRCC. Note particularly the information on course administration and other mechanics at the front of the NRCC. When you are ready, study the RTM pages listed in Assignment 1 of the NRCC, and go on from there. Good luck in your endeavor.

This training manual was prepared by the Naval Education and Training Program Development Center, Pensacola, Florida, for the Chief of Naval Education and Training.

Revised 1981

Stock Ordering No.
0502-LP-051-3262

Published by
NAVAL EDUCATION AND TRAINING PROGRAM
DEVELOPMENT CENTER

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON, D.C.: 1981

THE UNITED STATES NAVY

GUARDIAN OF OUR COUNTRY

The United States Navy is responsible for maintaining control of the sea and is a ready force on watch at home and overseas, capable of strong action to preserve the peace or of instant offensive action to win in war.

It is upon the maintenance of this control that our country's glorious future depends; the United States Navy exists to make it so.

WE SERVE WITH HONOR

Tradition, valor, and victory are the Navy's heritage from the past. To these may be added dedication, discipline, and vigilance as the watchwords of the present and the future.

At home or on distant stations we serve with pride, confident in the respect of our country, our shipmates, and our families.

Our responsibilities sober us; our adversities strengthen us.

Service to God and Country is our special privilege. We serve with honor.

THE FUTURE OF THE NAVY

The Navy will always employ new weapons, new techniques, and greater power to protect and defend the United States on the sea, under the sea, and in the air.

Now and in the future, control of the sea gives the United States her greatest advantage for the maintenance of peace and for victory in war.

Mobility, surprise, dispersal, and offensive power are the keynotes of the new Navy. The roots of the Navy lie in a strong belief in the future, in continued dedication to our tasks, and in reflection on our heritage from the past.

Never have our opportunities and our responsibilities been greater.

CONTENTS

CHAPTER		Page
1.	Management Techniques	1-1
2.	ADP Organization and Personnel	2-1
3.	ADP Physical Security/Risk Management/Privacy	3-1
4.	Systems Analysis	4-1
5.	Data Base Organization	5-1
6.	Worldwide Military Command and Control System Operations Community	6-1
7.	Documentation Preparation and Standards	7-1
APPENDIX		
I.	Life Cycle Phases and Policies	AI-1
II.	Users Manual, Computer Operation Manual, and Program Maintenance Manual	AII-1
INDEX		I-1

Nonresident Career Course (NRCC) Follows Index

CREDITS

Figures 6-2 through 6-19 and portions of pages 6-2 through 6-22 are reproduced through the permission of Honeywell Incorporated. Their courtesy and cooperation is gratefully acknowledged.

CHAPTER 1

MANAGEMENT TECHNIQUES

Good management traits and supervisory abilities are prerequisites for the First Class or Chief Petty Officer, who is required to function as a front line supervisor and manager. The DP1 or DPC will be in immediate control of personnel supervision and will have many management and supervisory responsibilities added to those present at the second class level. The supervisor should continuously MEASURE and EVALUATE the performance of the ADP facility in support of established management goals and objectives. For the purpose of this rate training manual, an ADP facility will be understood to mean the complete set of resources dedicated to meeting a command's requirements for automatic data processing ashore or at sea. It is not the intent of this rate training manual to set policy or direct any ADP facility in an authoritative nature. This manual will only make suggestions or show different approaches to common problems to assist the new DP1 or DPC in the requirements and responsibilities of the position. Various helpful authoritative publications, instructions, standards, and directives will be referenced throughout this manual. These references are cited for a purpose; "To assist you as a DP1 or DPC to gain a wider perspective of the data processing rating and assist you in pay grade advancement." The complexity of modern computer systems requires the DP supervisor and manager to have at hand a wide range of information to aid in effectively meeting the responsibilities of the position. These responsibilities range from satisfying the requirements of the "users," to notifying upper management of problems and status. A "user", in this instance, is anyone who requires the services of a computing system, ADP facility, or its products.

Having acquired a vast amount of valuable knowledge and experience within your field, it is now time to pass on this technical know-how to others. This chapter will discuss some of the various factors that will aid you in handling the supervisory and management duties and responsibilities of your job. Because the field is so vast, printed material on the subject so voluminous, and the scope of this text so limited, it gives you only a cursory glance at the various subjects. Your interest and dedication to the DP field should motivate you to seek additional information beyond this text and noted references. Remember, it is the dedicated, studious, and knowledgeable DP that will some day be called "Chief."

THE SUPERVISORY POSITION

To most people, it is a wonderful feeling to be promoted to a supervisory position. Most people like the feeling of added prestige, authority over others, and the feeling of progress that goes with promotion. Of course, that increase in pay adds to the general good feeling, too.

Supervision involves working with people, and a major responsibility of a supervisor is production. A good supervisor knows how to get a job done by getting the most out of personnel. As a word of caution, however, the drive for production must not overshadow the consideration for the human element. People are not machines, and if you treat them as such, you will find that no amount of pressure will permanently increase the production rate. While you want to achieve a high level of production, you also want your personnel to produce willingly and to show an interest in their work.

If you have even a small amount of experience in supervising others, you are perhaps well aware that the job of supervisor is not as easy as it might sometimes seem. The following discussion will present some of the major factors involving the supervisory position.

COMMON MISTAKES

In learning any job, learning what NOT to do is often as important as learning what to do. The following are some common mistakes which new supervisors tend to make, and which a new supervisor should avoid.

Your first days as a new supervisor are important. Your personnel will be watching to see how you react to this new responsibility. Your superiors will be observing you, too. This is the period to avoid some of the common mistakes made by supervisors.

"New broom" tactics are out! It is not unusual to see an inexperienced supervisor go into a new job with the idea that "things are going to be different around here." A new supervisor wants to make a big showing, or let it be known that the way the last supervisor operated is now unacceptable. This precludes a very potent psychological factor called "resistance to change." People fear and resent change. It is far better to let your personnel know that nothing will be changed for the time being; and, after you get your feet on the ground, gradually make the necessary changes.

Do not make promises in order to gain friendship and support. Even a hinted or implied promise can sometimes be dynamite.

Avoid dictatorial practices; they are fiercely resented. An overshowing of authority during your first days on the job will be particularly noticed.

Careless remarks, which would go unnoticed if they came from one of the crew, take on a new significance when they come from a supervisor. You must carefully weigh your remarks when members of your shop or crew are listening.

Failure to delegate work and fearing to trust subordinates are common failings of a new supervisor. The result is that soon the new DPs work gets stacked up and the whole unit is bottlenecked.

When you make a promise and are unable to keep that promise, you accept the blame. There may be a good reason for your inability to keep your promise or the fault may lie with one of your subordinates, but the important thing is that you accept the responsibility and do not pass the buck. Passing the buck when something goes wrong is a sure way to lose the respect of your subordinates. And above all, do not lose your temper in front of your personnel. You must be master of yourself before you can control others.

THE FINE LINE

As a supervisor, you must draw a fine line in the relationships between you and your crew. Do not assume a false dignity; but at the same time, the old "buddy-buddy" relationships that you used to enjoy are no longer appropriate. Drawing this fine line is one of the most difficult parts of the job of a new supervisor, but it must be drawn. It is understood that the first class who is the shop supervisor or crew leader has the more difficult job in drawing this fine line, especially when on duty. The team leader eats and sleeps with other data processing personnel. The new DP1 also attends the same clubs, but must ensure that subordinates understand that general conversation in the relaxed atmosphere of the club and comments on the job carry different weights and have different values. While this does not mean that a supervisor's actions on the job are to be radically different from those off duty, it does alter some measure of relaxation.

To accomplish this task and maintain balance, ask your subordinates for advice and help, rather than give the impression that you know it all. Let the crew know that you have confidence in them; maintain a friendly but conservative attitude; treat them all alike; be consistent; and set a good example yourself.

SUPERVISORY DUTIES AND RESPONSIBILITIES

A specific list of duties and responsibilities can be made only when it concerns a specific

position; however, here are some typical duties and responsibilities:

1. Getting the right person on the job at the right time
2. Using and storing materials economically
3. Preventing accidents and controlling hazards
4. Keeping morale high
5. Maintaining the quality and the quantity of work
6. Keeping records and reports
7. Maintaining discipline
8. Planning and scheduling work
9. Training personnel
10. Procuring the supplies and equipment to do the work
11. Inspecting, caring for, and preserving equipment
12. Giving orders and directions
13. Maintaining liaisons with other units
14. Checking and inspecting jobs and personnel
15. Promoting teamwork
16. Maintaining good housekeeping on the job
17. Keeping operations running smoothly and efficiently

Analyzing the typical duties and responsibilities listed above, indicates that the following major areas are common to all supervisory positions:

1. Production
2. Safety, health, and physical welfare of subordinates
3. Development of cooperation
4. Development of morale
5. Training and development of subordinates
6. Records and reports
7. Balanced supervision

These areas of responsibility will be discussed in the following paragraphs.

Production

It is the supervisor's responsibility to see that all work is done properly and on time. This is true in the office or in the shop. To accomplish those jobs, the supervisor functions in three main ways:

1. The work must be organized and planned so that maximum production is accomplished with a minimum of effort and confusion.

2. As much as possible, the responsibility and authority for completing the work must be delegated, keeping in mind that the final product is the responsibilty of the supervisor.

3. The supervisor must control the work load and see that all work is prepared correctly.

Safety, Health, and Physical Welfare

Safety and production go hand in hand. The safe way is the efficient way. When personnel are absent because of injury, they are non-producers. A good supervisor stresses safety to the crew; sets an example by working safely; teaches safety as an integral part of each job; and most of all, plans each job with safety in mind. A good supervisor does not wait until after an accident happens to start safety measures.

Showing concern over the health and physical welfare of your crew will also pay off in increased production. It will add to their feeling of trust and confidence in you as a supervisor and increase the amount of respect they have for you.

Development of Cooperation

The necessity for developing cooperation between the members of a supervisor's own unit goes without saying. Some supervisors, however, tend to overlook the necessity for cooperation in two other directions:

1. Cooperation with management
2. Cooperation with supervisors of other units

In carrying out the job, a supervisor often has dealings with persons in other units of the activity. It is particularly essential, therefore,

that supervisors of these units develop the cooperation listed in (1) and (2) above.

Development of Morale

The esprit de corps of a group and their willingness to work toward common goals depend to a great extent upon the leadership of the supervisor. A producing group will be found to be a group with high morale.

Training and Development of Subordinates

A good supervisor is invariably a good teacher, and a good leader is a developer of men and women. One of the basic policies of Navy supervision reads:

The greatest contribution supervisors can make is the development of their people. A good supervisor will arrange to have at least one trained person ready to assume responsibility should the need arise. It is a sign of good leadership when a supervisor can take leave, and the job continues to run smoothly. Do not be afraid to teach every phase of your own work to at least one or two subordinates. A great deal of the supervisor's time involves teaching, so cultivate your teaching ability.

Reports and Records

Most supervisors, particularly shop personnel, do not like to keep records and prepare reports, yet they are a vital part of the work. Make it a point to keep neat, accurate records and reports, and get the reports in on time. Paperwork may look like a waste of time to you, but some day you will realize how much your job depends upon it. Some required reports and reporting procedures will be discussed in the management portion of this chapter.

Balanced Supervision

Analyze the major duties and responsibilities just covered. You, as a supervisor, must pay proper attention to each phase of your job. Do not emphasize production at the expense of safety or training. Also, do not become so concerned with the human element that production is neglected. Keep up with paperwork, and in so doing avoid its accumulation to the extent that you have periods when you have to devote your entire interest to this responsibility at the expense of others. Always strive to put the proper emphasis on each of your responsibilities and you will be practicing balanced supervision.

TRAITS OF A GOOD SUPERVISOR

There are various traits that are desirable in a supervisor. Some of these traits are discussed below.

Loyalty

One trait that should stand out in every supervisor is loyalty. It is important that you show loyalty to your country, to the Navy, to your unit, to your superiors, and to the people who work for you. Surely, you will agree that to get the respect and loyalty of your personnel, you must be loyal yourself.

Positive Thinking

A good leader will always be a positive thinker. Thinking in terms of how things can be done, not why they cannot be done. The positive thinker maintains an open mind to changes, new ideas, and training opportunities, looking to the future with confidence, a confidence that is catching. Everything worthwhile that has ever been accomplished in this world was accomplished by positive thinkers. If you want to lead others, start today and practice the art of positive thinking.

Genuine Interest in People

Have you ever met really great leaders? If so, instead of being cold, and aloof, this individual, probably turned out to be a warm, friendly, human being who seemed to make you feel important by paying close attention to your words.

One of the first steps you, as a new supervisor should take is to get to know your

people personally. This not only creates the feeling of genuine interest in the individual, but helps you to place the right person in the right job at the right time.

The importance of knowing your crew personally increases when the need arises to convert from a data processing technician to a professional defensive tactician and fighter. Here, the wrong person in the wrong place could prove disastrous.

INITIATIVE

A person with initiative is always needed in the naval service. Initiative is evidence of an open and alert mind. If you have initiative, you continually look for a better way to do things; you do not wait for others to do them. You do not put off until tomorrow what should be done today. If you see an unsafe condition, you correct it before an accident occurs. If you see that a new form or procedure would simplify the job, you devise it. If you see an inadequacy in yourself, you sincerely try to overcome it. A weak person lacks initiative. A leader is characterized by strong initiative.

Decisiveness

A leader is able to make decisions. One of the most common complaints heard from subordinates is, "You can't get a decision from our supervisor."

A great majority of the decisions that have to be made by a supervisor in the naval service concern relatively petty things. As often as not, the person merely wants the supervisor's approval to perform some minor action which the individual already knows should be done. A prompt "yes" from the supervisor is all that is necessary. In many trivial matters it makes little difference whether the answer is "yes" or "no." The important thing is to get an answer. The supervisor who stalls, puts off, evades, or refuses to give a decision is a bottleneck.

Of course, there are times when a decision requires careful consideration of many factors and therefore much deliberation. In such cases, the supervisor should tell the person when to return for the decision and see to it that the decision is ready when promised.

Tact and Courtesy

A good leader is habitually tactful and courteous. Whether in the shop or office, a supervisor can be courteous. Being courteous does not imply that a supervisor is a weakling or a sissy; rather, it implies thoughtfulness.

Tact can be defined as "saying and doing the right thing at the right time." It is the lubricating oil in human relationships. It is the regard for the feelings of others based on an understanding of human nature–the little considerations that make the job pleasant and smooth.

Courtesy can be defined as "treating others with respect." It means treating people as important human beings, not tools to be used for your convenience. It means following the accepted rules of conduct, being polite. Courtesy is one of the marks of a good supervisor. Courtesy is important to the supervisor. One discourteous act, even though unintentional, can make you an enemy–and, as a supervisor, you cannot afford to have enemies. "If you have one enemy, you have one too many." Remember, courtesy is contagious.

Fairness

The personnel in a shop or crew are extremely sensitive to partiality by the supervisor. They will even single out little incidents where there was absolutely no intent to show favoritism. For this reason, you must think ahead on changes to be made, decisions to be handed down, work assignments, recommendations for promotion, and the like. In each instance you must say to yourself, "This action will make this particular individual happy, but how will every other individual in my unit feel about it?"

Many experienced supervisors will tell you of cases where they were very friendly with certain individuals, when the time came for discipline or some other adverse action, it was very difficult to deal with the situation.

Sincerity and Integrity

A supervisor who deals with personnel squarely and honestly all the time, wins and

holds their respect. Such a supervisor can talk with crew members on a one-to-one basis, and not be afraid to face the facts. "Give me the supervisor who looks you straight in the eye and tells the truth every time!"

Consistency of thought and action are important if the crew is going to know where they stand. Being too strict one day and too lax the next is worse than being consistently strict or consistently lax. It is not wise to exhibit good and bad moods to your crew. Strike a happy medium between firmness and laxness and be consistent.

Dependability, one of the marks of integrity, involves meeting obligations promptly. A reputation for being a "square-shooter" is worth every effort on your part. This reputation must be built early, even prior to appointment as a supervisor. One violation of integrity may take months to rectify—or forever.

Confidence

A good supervisor has a quiet confidence (not an arrogant or cocky manner) based on a thorough knowledge of the job and a belief in personal ability. Confidence begets confidence. The mousy, hesitant supervisor who lacks personal confidence, cannot inspire confidence in others. It is amazing to see how people will follow an individual who is charged with confidence personally and in an idea. Even crackpots or cranks can win followers if they appear confident. Some people put on a front of aggressive confidence to hide an inferiority complex. They ridicule the opinions of others; they dominate conversations; they are arrogant. Such individuals get their come-uppance sooner or later. However, the individual who has quiet inner confidence, expressed by a confident manner, by actions, and by words, is respected and followed.

MAINTAINING DISCIPLINE

One of the major problems which you as a new supervisor may encounter is that of maintaining discipline of subordinates. The following discussion provides some pointers that will help you achieve success in maintaining discipline of those under your supervision.

The Art of Giving Orders

A good supervisor gives much thought to the art of giving orders. Proficiency in this area reaps many benefits, and since most disciplinary problems are the result of the failure of people to carry out orders, this subject cannot be overemphasized. There are three basic types of orders:

1. The command
2. The request
3. The suggestion

Consideration should always be given to (1) the situation under which the orders are to be given, and (2) the individual who is to carry out the orders. Succeeding paragraphs examine the types of orders listed above in the light of each of these two considerations.

The Situation

In military formations, the direct command, or formal type of order, is always used. The direct command should also be used when there is immediate danger, a fire, an accident or other emergency, disobedience of safety rules, and so forth.

The simple request is the best type of order to give for daily routine work. The request is used for most orders given by good supervisors.

The suggestion is excellent when you wish to use personal initiative, when you do not have time to work out the details, or when you do not know yourself exactly how the job should be done. This method of giving orders builds morale and shows your people that you have confidence in them. However, it is not clearcut, and you certainly would have no recourse if the job were not done properly.

The Individual

The direct command might have to be used in giving orders to the careless, lazy,

insubordinate, or thick-skinned individual. Except in the unusual situations mentioned above, the direct command is normally reserved for those to whom we must speak firmly and positively.

The request is by far the best type of order to use with a normal individual. With most individuals, a simple request in the form of a question has the full effect of a direct order. Moreover, it fosters a feeling of cooperative effort, of teamwork.

The suggestion is excellent for those to whom a suggestion or hint is sufficient. Individuals with real initiative like to be "put on their own." In dealing with a sensitive, highly intelligent individual, a mere hint that something is desired is enough to get a project started. For example: "Petty Officer Smith, I wonder if it would be a good idea to do this?" or, "Do you have any ideas on how this can be done?" or, "One thing we really need is . . . ". Petty Officer Smith then becomes a key person in the project and feels important. It shows your confidence in Smith as an individual, and thus provides excellent training. The suggestion type of order stimulates an individual's personal performance.

Although the situation and the individual are the prime considerations in giving orders, the attitude and tone of voice in which they are given are very important. Give all orders in accordance with the five "C's"–Clearly, Completely, Concisely, Confidently, and Correctly. Also avoid orders that are unnecessary and/or superfluous.

THE ART OF REPRIMANDING

When an order is disobeyed or not carried out, you would be remiss in your duties as a supervisor if you did not do something about it. The most common type of discipline used by supervisors is the simple reprimand.

The reprimand, too, must be fitted to the individual and the situation. Just the slightest hint of something wrong will be more crushing to a sensitive individual than the severe rebuke you might give a thick-skinned person.

The reprimand should be a calm, constructive action, not a destructive one. You are interested in building strong individuals, not tearing them down. You are interested in the underlying cause(s), not in how to get even with an individual.

Failure to act when a reprimand is due is a sign of poor supervision. A supervisor should not be too lenient and ingratiating. If one of your crew "gets by" with something, you may lose control. Issuing too many reprimands is just as bad: an inexperienced school teacher, for instance, may keep scolding pupils until complete bedlam results!

A fine line should be drawn between harshness and leniency. Only a supervisor with a keen understanding of human nature can discern this line.

Practice the three "F's" of discipline: Fairness, Firmness, and Friendliness. The recommended procedure for administering reproof follows:

1. Get all the facts.
2. A person should not be reprimanded in front of others.
3. Put the individual at ease. Give a word of praise first, if appropriate, to take out the sting.
4. Use no sarcasm, anger, or abuse.
5. Fit the reprimand to the individual.
6. Have all the facts at hand; there may be an attempt to deny the charge.
7. Present the facts.
8. Ask the person why there was an error.
9. Try to get the person to admit to the mistake.
10. Do not threaten; the individual knows how far you can go.
11. Once there is an admission of guilt, the reprimand is over.
12. Leave on a friendly note, letting the person know the incident is closed. Do not nag.
13. Later, follow up with a casual and friendly contact at the shop.

To test the effectiveness of your reprimand, ask yourself, "Did it build morale?" Remember that you must get along with subordinates in the future; you must keep them working, a producing unit; and you must be able to get

along with your own conscience. You do not have to be soft, but remember that there is a great deal of difference between dignity and arrogance.

POSITIVE AND NEGATIVE DISCIPLINE

So far, discipline has been spoken of in terms of punishment. Actually, discipline is much more than reprisal for wrongdoing. Discipline exists also where no disciplinary actions ever have to be taken. Most people realize that they cannot get along without self-discipline, and that no organization can function, no progress can be made, unless individuals conform to what is best for the whole group. The supervisor who can build the spirit of cooperation, which is the basis for true discipline, has no discipline problem.

Positive discipline, the trend in discipline that is being studied widely by intelligent executives and supervisors, is the force that originates within the person that prompts obedience to rules and regulations. People in a Navy organization do what is right because they do not want to hurt the group as a whole, and because they believe that by following the accepted rules the group's objectives will be accomplished. The supervisor who builds up this esprit de corps has little need to resort to negative discipline. Negative discipline is a discipline of fear, based on threat of punishment. This type of discipline originates from without the person. An individual subjected to this type of discipline will do only enough to get by when you are watching. When you leave for a few minutes, discipline leaves too. The individual's only motivation for working is fear of reprisal.

Discipline and high morale go hand in hand. Positive discipline is closely tied in with the admiration and respect of the people for their supervisor. This, in turn, is based on good human relations.

THE HUMAN RELATIONS ASPECT OF DISCIPLINE

When good human relations exist between you and your work force, it is usually an indication that you appreciate and understand your people, have their interests and welfare at heart, and respect their opinions, knowledge, and skills.

Some of the human relations factors that lead to positive discipline are listed below:

1. As a good supervisor, you should understand the principles, standards, rules, and regulations necessary to good conduct. Believe in these things and practice them yourself.

2. Know your people as individuals, and treat them fairly and impartially.

3. Develop the feeling of "belonging" and security in the group.

4. Get information to the group through proper channels, and promptly eliminate rumors.

5. Use authority sparingly and always without displaying it.

6. Delegate authority as far down the line as possible.

7. Never make issues of minor infractions or personal issues of disciplinary matters.

8. Display confidence in the group, rather than suspicion. (Workers are reluctant to betray expressed confidence.)

9. Train the group technically.

10. Look after the mental and physical welfare of the group.

11. Try to avoid errors, but show willingness to admit errors when they are made.

12. Develop loyalty in the group and of the group.

13. Know that idle hands or minds lead to trouble, so keep them busy. (Slack work periods can be used for training.)

14. Know that because of individual differences discipline cannot be a completely routine matter. Discontent, idleness, lack of interest in the job, misunderstanding of regulations, lack of uniform enforcement of regulations, resentment, and emotional strain are some of the principle causes of misconduct. The wise supervisor will avoid the necessity for formal discipline by removing as many of these causes as possible.

ACHIEVING TEAMWORK WITHIN YOUR OWN GROUP

Since primitive times people have learned to band together for protection, to build, or to attain a goal too large to be accomplished by an individual. They have learned that in unity there is strength. There are also psychological factors involved and every supervisor should know and appreciate these psychological rewards that a group must give to hold its members:

1. A feeling of security
2. A feeling of "belonging"
3. A feeling of "being somebody" within the group
4. A feeling of pride in the group
5. A feeling of recognition from outside the group (The harder it is to get into the group, the more important the members feel.)
6. A feeling of accomplishment (The group is attaining common goals.)
7. A satisfaction of certain needs (advancement, pride in work, acquiring new skills, and so on) while attaining the goals of the group.

A good leader will encourage these feelings, since the stronger these psychological rewards, the stronger will be the group. Some supervisors achieve such a strong feeling of group pride that their crew actually feel that it is a privilege to work in the group. The people we supervise are human beings with individual differences, and they usually produce only to the extent that they feel like producing; and their will to produce is based primarily on the ability of supervisors to win their cooperation. Good leadership is reflected in this ability to get cooperation; and cooperation, in turn, is a reflection of the respect the people have for their supervisors. Teamwork or cooperation, then, is based on good human relations.

When you walk into any shop or office, you can almost feel whether or not the spirit of cooperation is present. If it is there, you can see it in the faces of the people, in the appearance of the work spaces, in the reception you receive, in the way the work is performed.

Poor cooperation is indicated whenever bickering, jealousy, and friction, are present. Low production is the inevitable result. Frequent accidents, indifference, sloppy work, griping, complaints and grievances, criticism of the unit, buck-passing, loafing, many requests for transfer, poor planning, poor training or indifference to training–all these danger signals indicate lack of cooperation.

ELEMENTS TO CONSIDER IN DEVELOPING COOPERATION

Developing cooperation within your group is largely a matter of adapting your behavior to meet the varying situations encountered daily–and in going out of your way to show a willingness to cooperate. You do not just order cooperation! You achieve it.

Correcting Mistakes

When correcting a mistake a crew member is making, unless safety is involved, make the correction through those who deal directly with the individual. There may be a valid reason for the performance of what you may consider to be a mistake. Remember, the individual takes orders from an immediate supervisor, and this supervisor may have a valid reason for making changes to your orders.

Delegation of Authority

A good supervisor soon learns to delegate work, developing subordinates and getting them to do all the routine work. Such a supervisor then has time to handle personnel problems, time to study, and time to do the necessary planning and creative work. The supervisor who does not learn the knack of delegation, develops ulcers–and a noncooperative group!

Keeping Your People Informed

Keeping your people informed means exactly that. It is extremely important that your people know the reasons "why" regarding changes that affect them. If security prevents

you from giving reasons, tell your people. Remember, "Morale does not well up from the bottom—rather does it trickle down from the top!"

Setting the Example

It is your job to set the example. If you are enthusiastic about your job, friendly and good-humored, and foster harmony among your associates, you will attain your goals and do much to create a cooperative attitude in your group by your personal example.

Giving Credit

Do not fail to give credit where credit is due, and do not forget to pass on any credit given to you. A good supervisor gives full credit to the team. Frequent and sincere praise is a wonderful incentive to individuals and to the group as a whole.

Tactful Handling of Personal Problems

Personal problems come up almost daily in any group of people. A supervisor must tactfully handle each of these. Rumors about any of your people, disputes between the workers, family troubles, and similar situations can disrupt the efficiency of the group. Usually positive action by you is required.

You, as a supervisor, should try to solve problems that arise in your shop or crew that are within your capability of solving. This does not mean that you should act as chaplain, marriage counselor, and/or psychiatrist, rather it emphasizes the need to be able to recognize the symptoms of those problems requiring special ability in solving, so that you may arrange to have them placed in proper hands as soon as possible.

In each case, you must first listen and get all the facts, then tactfully bring about a solution so that all concerned can go back to the job and work in harmony. Facing problems squarely and honestly, bringing them out into the open on a personal basis, and solving them before they explode, are usually the best courses of action.

COOPERATION WITH YOUR SUPERIOR

Your superior is very important to you. In this individual's hands rests much of your ability to successfully complete your job.

Many supervisors rate loyalty as the most desirable quality in an employee. As a loyal supervisor yourself, it is your duty not to criticize your superiors to others, even when you do not agree.

Dependability is another desirable quality your superior looks for in you. Your boss likes to know that once an assignment is given to you, it will be carried out to completion to the best of your ability, and on time. There are few things more annoying than the person who always has an alibi—who cannot be depended upon.

Do not be a "yes" person, but on the other hand, do not go to the extreme of being a "no" person. Your superiors want subordinate supervisors who are not afraid to state opinions tactfully, even if this means opposing opinions. This does not mean, however, that you should disagree constantly and consistently oppose every idea!

Make Suggestions Tactfully

Most bosses resent employees who make it a common practice to tell them bluntly what should be done or what shouldn't be done. It's easy to get your ideas across to the boss without incurring resentment; just put them in the form of a question: "What do you think about this idea?" or "Do you think this would work?" If your supervisor gives you an assignment that is obviously a mistake, tactfully inquire about handling it in another manner. However, if your supervisor insists, do not argue.

Keeping the Boss Informed

Your boss likes to know what is going on, but he does not want to be bothered with all the petty details. Keep your boss advised of personnel problems, proposed changes, and other important matters.

If you make a serious mistake, tell your superior about it immediately, rather than wait

for it to be discovered. Remember also, your superior will not want a lengthy explanation of your actions.

COOPERATION WITH YOUR FELLOW SUPERVISORS

Friction and jealousy are your prime enemies in establishing a feeling of cooperation with your fellow supervisors. It is the good supervisor who avoids "back-stabbing," gossiping, or criticizing fellow supervisors when the competition becomes keen. The big thing to remember is that you do not rise by crushing others. Eventually unkind actions will boomerang, and if enough people dislike you, you will start failing in your job.

In addition to being cooperative personally, a good supervisor may sometimes have to encourage cooperation on the part of other supervisors. In the long run, it is the person who is able to foster and maintain harmony in all relationships who is needed for the Navy's key jobs.

THE MANAGER POSITION

The first part of this chapter has dealt with the supervision of personnel. As a DP1 or above, a good portion of your time will be taken up in the technical management of the ADP facility. The data processing technical manager, usually a DP1 or above, is responsible for carrying out the objectives set forth by higher authority. The technical ADP manager must have the authority to accomplish the responsibilities of the position and must have the complete cooperation of all other levels of management in performing job-related duties. In accomplishing the objective of the ADP facility, the technical ADP manager must keep upper management informed of the progress made, as well as many problems which may arise.

Although the procedures for ADP equipment vary according to the purpose for which the equipment is to be used, problems of management are quite similar among all ADP installations. No Navy activity using ADP equipment is relieved of the tasks of applying the most economical contract terms, assuring proper computation of rental and maintenance costs, accurately recording time, effectively using the equipment, and all the other aspects of good management.

All Navy activities that have an ADP facility should establish or have a reasonable replica of a Computer Performance Management (CPM) program. A CPM program is any structured effort that measures and evaluates the performance of installed computer systems in support of established local upper management goals and objectives. This subject area is suggested to assist the DP1 and above in planning and organizing a CPM program at all Navy ADP facilities. The following paragraphs provide an explanation of the relationship between CPM and the functional responsibilities of the ADP facility DP technical manager. Specific responsibilities to be considered include: (1) service to users; (2) management of resources; (3) communication with upper management and higher authority; (4) vendor and Customer Engineer (CE) relations.

CPM AND MANAGEMENT RESPONSIBILITIES

The problems and responsibilities that the ADP technical manager must face are similar to those encountered by petty officers in other functional areas of any command. The goal of maximizing productivity at minimum cost applies to the DP technical manager as well as the manager of the engineering spaces of a carrier. The BT or EN petty officer's need for timely and accurate information with which to plan for future requirements is as acute as the needs of the DP technical manager of an ADP facility. But while the growth of computer technology has helped to ease the burden and increase the effectiveness of managers in nearly every other aspect of command operations, it has sometimes turned the ADP facility technical manager's job into an overwhelming challenge. The DP1 or above may be charged with the responsibility for technically managing a multimillion dollar resource ashore or at sea that operates at electronic speed on hundreds of

independent problems at a time. The Navy's largest computers can process thousands of different jobs, from as many different sources, each day. Except for sporadic messages on the operator's console, and the visible movement of tapes, disks, and printers, most of what determines how well a computer system does its work is concealed within the circuitry of the hardware itself. It cannot be observed, measured, or evaluated without the application of specialized technology. Yet many of the important decisions that a DP must make about the ADP resource depend upon a detailed and precise understanding of these invisible events and what they signify.

Consider a few of the decisions that the ADP facility technical manager faces nearly every workday.

1. Are user complaints about poor service justified?

2. If so, what is the most economical and feasible way to remove or minimize the cause(s)?

3. If not, what kind of human factor may have led to user dissatisfaction and how should the facts about service levels be communicated to the user?

4. What improvements could be realized by minor modifications to user requirements?

5. How are user requirements expected to change in the next 1 to 5 years, and with what affect on present resources?

6. As for the facility itself, how many operator shifts are needed to handle the existing workload?

7. How should the computer room be laid out to optimize operator efficiency?

8. What kind of background should be required of support and operator personnel, and what kind of training should they receive after they arrive?

9. Is the amount of downtime the system suffers reasonable, given the state of contemporary hardware electronics and software engineering?

10. Is the apparent slowdown in throughput during prime time hours (0700 to 1600) acceptable to users? To upper managment?

11. Is there anything that can be done with the present configuration to enhance its performance during prime hours?

12. If so, will the benefits justify the cost of the enhancement?

13. If not, where is the bottleneck in the system and what is the most cost-effective way to alleviate it?

Questions like these could fill the entire DP1 and DPC rate training manual. The point is that having reasonable and well-documented answers to these questions largely determines the effectiveness with which a DP manages an ADP facility, instead of merely supervising it. The fact is that good supervision and good management go hand-in-hand in the control, operation, and financial budgeting of an ADP facility. The answers to the preceding questions will provide the Navy with substantial dollar savings, or significantly enhance a command's ability to carry out its mission. The most immediate objective of a CPM program is to maintain control of a complex, costly, and critical resource through a thorough understanding of how that resource performs. Supervisors and managers must be aware of the alternatives that are available to make the program perform more effectively and efficiently.

User Requirements

ADP management's greatest responsibility is to its user. They are the reason the ADP facility exists and the reason you, as a DP, are stationed in the billet at your parent command. Although specific user needs cannot be stated for every command, several categories of user requirements do appear to be common at all ADP facilities. These common requirements are (1) timeliness (2) accessibility (3) reliability and (4) availability. These requirements are discussed in the following paragraphs.

TIMELINESS.–Most ADP users have deadlines to meet and rely on the computer to

help them to meet these deadlines. This is as factual during a project's research and development phase as it is in the production phase, and is reflected in the user's need for rapid turnaround time. In order to meet these system demands, the ADP technical manager must know all system turnaround time requirements, and whether the ADP facility is meeting these. Personally surveying users is not a practical approach to defining such requirements and waiting for the user to complain is no solution for monitoring levels of service. The ADP technical manager should obtain detailed information from system accounting log files for each job class. This entails the number of jobs submitted and the percentage of jobs meeting predetermined turnaround times. This type of information is invaluable in resolving questions about batch job turnaround time while the job is actually in the system. (See figure 1-1.) If a critical delay is outside the system, the production control logging procedure should record actual batch job submission and pickup times, and should include manual operations such as reading in cards, bursting output reports, pulling input tapes, etc.

Although degradation of turnaround time by a few seconds is not noticeable to the mainframe batch user, an equivalent delay in response time can be very irritating to the remote batch processing (RBP) unit or remote terminal (RT) user. The development of system software has made it possible to accurately measure RBP and RT response time at a large number of ADP facilities. From management's view this information is very helpful.

ACCESSIBILITY.–The location and quantity of remote batch processors and remote terminals can do much to affect a user's attitude toward an ADP facility. A user who has difficulty in finding an unused terminal will have little regard for the ADP technical manager's efforts to satisfy immediate requirements. Measurement techniques can be used to record the port numbers and sign-on IDs of every remote access to the mainframe Central Processing Unit (CPU). The ADP technical manager should analyze this data and make suggestions to upper management for a more balanced placement of available terminals, if needed.

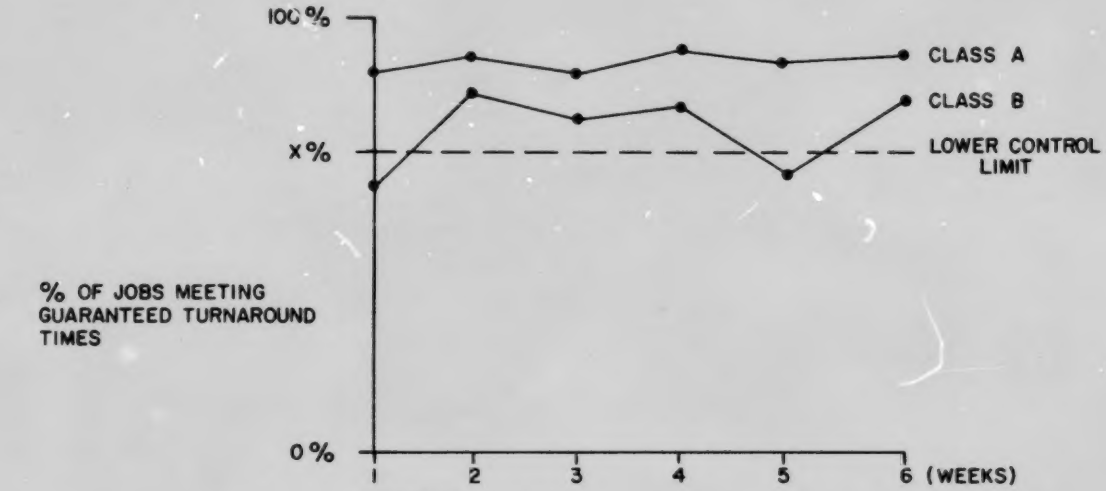
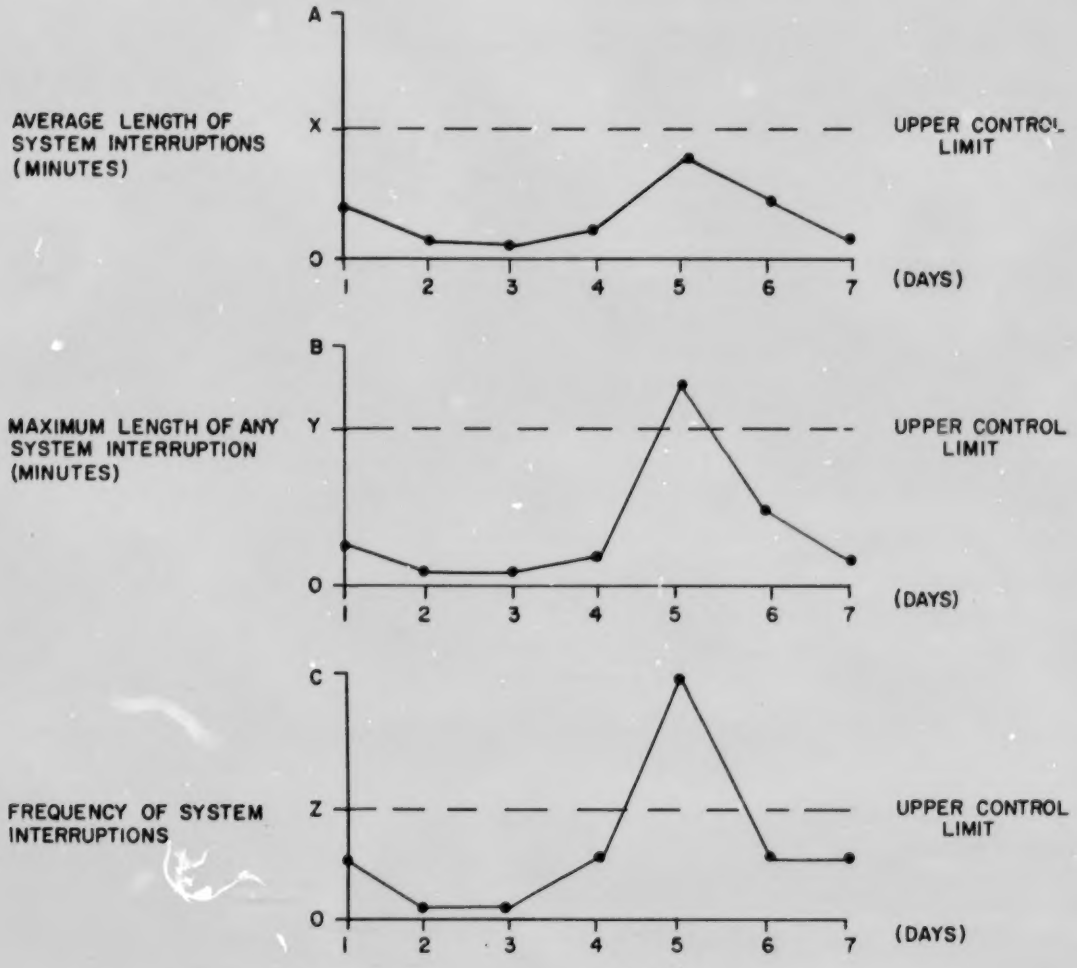

100 %
X %
0 %
CLASS A
CLASS B
LOWER CONTROL LIMIT
% OF JOBS MEETING GUARANTEED TURNAROUND TIMES
1
2
3
4
5
6 (WEEKS)
FREQUENCY: WEEKLY
PERFORMANCE CRITERION:
1. X% OF ALL JOBS IN EACH CLASS SHALL SATISFY THE GUARANTEED TURNAROUND TIME REQUIREMENTS OF THAT CLASS.
NOTE: A CONTROL LIMIT IS A VALUE CHOSEN BY THE ADP TECHNICAL MANAGER AND UPPER MANAGEMENT, TO REPRESENT THE BOUNDARIES OF AN ACCEPTABLE PERFORMANCE FOR A PARTICULAR SYSTEM VARIABLE.

Figure 1-1.–Sample turnaround time report for management.

RELIABILITY.–A brief system crash (software or hardware abort) may have little impact on the total turnaround time of a batch user's job, but it is unnerving to a user sitting at a remote terminal wondering when the system will come up again and how much work may have been lost in the process. Without sufficient information as to the frequency and duration of system crashes, the ADP technical manager has no real feel for the quality of service that is being provided to the users. Simple logging procedures such as mean time between failures (MTBF) and mean time to repair (MTTR) can provide this information. Figure 1-2 is a sample



FREQUENCY: DAILY

PERFORMANCE CRITERIA:

1. THE AVERAGE LENGTH OF SYSTEM INTERRUPTIONS SHALL BE LESS THAN X MINUTES.
2. NO INTERRUPTION SHALL LAST LONGER THAN Y MINUTES.
3. THERE SHALL BE NO MORE THAN Z INTERRUPTIONS PER DAY.

Figure 1-2.–Sample report of system reliability for upper management.

report for upper management showing the reliability of the system.

AVAILABILITY.–System availability is usually defined as the percentage of scheduled and unscheduled time during which the computer system is operational and available to the users. There is another aspect of availability, however, which concerns the nature of scheduled time itself. Complete system dedication for a single purpose should be avoided during prime work hours, if at all possible. Information concerning the magnitude and types of demands covering several weeks can be used to determine the appropriate hours of scheduled time for each user or project.

SCHEDULING

Scheduling is one of the most important and difficult jobs of an operating installation. Schedules should be tight enough to preserve valuable machine time, yet flexible enough to allow for set up time, manual operations in case of errors, and unavoidable delays. Scheduling requirements will generally be determined by the characteristics of an installation. The following cases present two extremes:

1. An installation that operates within rigidly prescribed standard application

2. An organization that provides service for a multitude of users

Most installations fall somewhere between these extremes, and the scheduling must be tailored to meet the needs of the particular installation. Operating under rigidly prescribed standard applications normally ensures a relatively fast turnaround. With a multitude of users the turnaround time depends on the total workload, and the distribution of this workload. To do an effective job of scheduling, the schedule must be realistic. A realistic schedule allows for buffer periods. The basic reason for buffer time involves the required coordination in time of several activities in a data processing run. Perfect coordination of all activities cannot be expected.

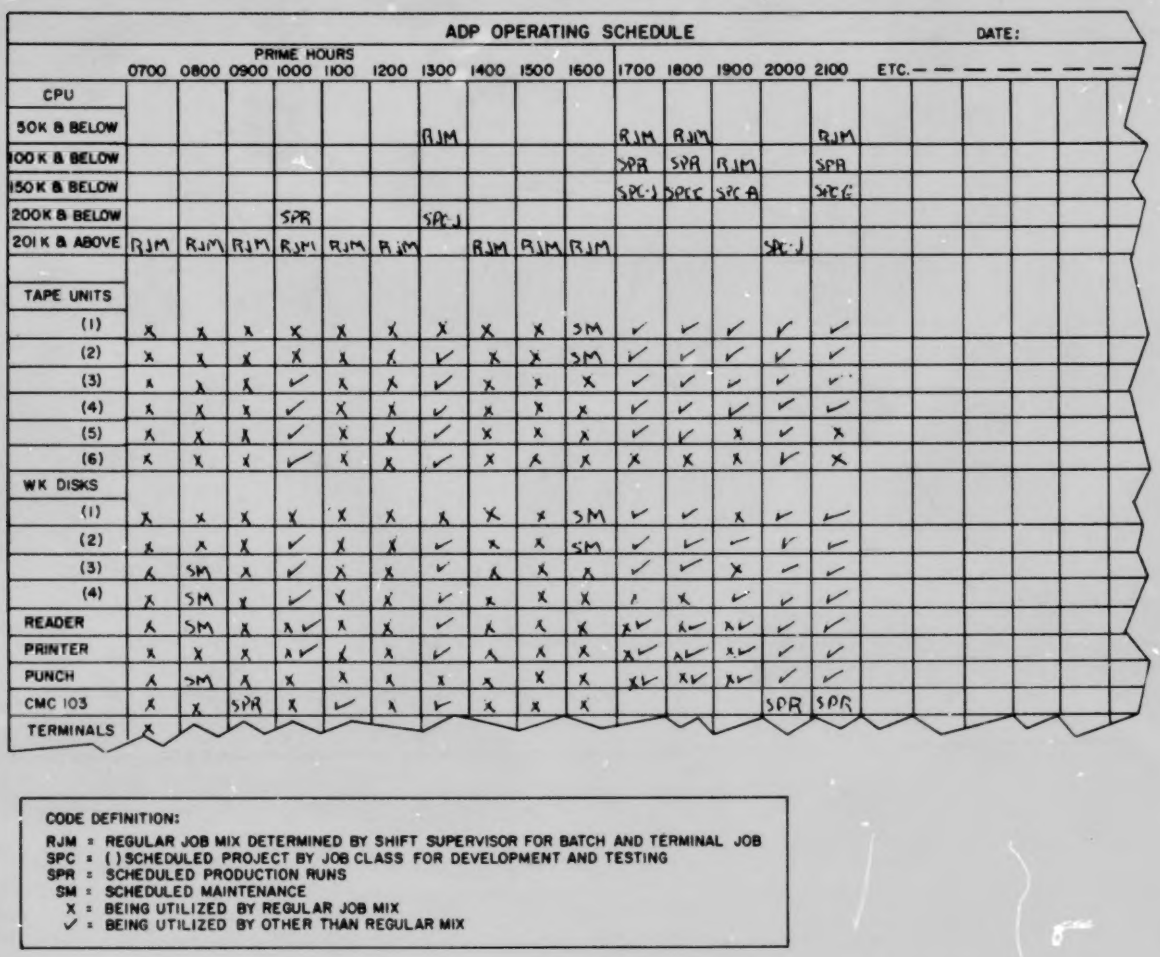
The value of scheduling specific time for program testing has been proven by experience. A continuing need for test time is evidenced by the development of new applications, and maintenance and improvement of existing programs.

To keep setup time to a minimum, optimum scheduling must be employed. Also useful in minimizing setup time is intelligent programming which keeps to a minimum the number of changes of tape reels, disks, and other peripheral equipment.

A typical example of a daily operating schedule is shown in figure 1-3. The average computer task is 30 minutes or less. Scheduling in one 1 hour blocks allows for special setup time, buffer time, and a good mix of other tasks. This schedule shows 24 hours across the top. Auxiliary, remote, and system components are shown in the left margin. The codes in the time blocks will let the operating shift supervisor plan the job mix on the system with a reasonable degree of advance planning during the day. For better turnaround time and testing for the user, as much of the system as possible should be left open during prime working hours for regular job mix, remote batch processing and remote terminal use. However, this will not be possible 100 percent of the time.

In addition to scheduling testing time, all production runs must be scheduled to ensure utilization of the equipment. In the case of standard runs, they should not exceed certain set limits on input/output (I/O) and running time. Reasonable limits can be determined only through a study of the systems environment. For instance, do all applications utilize all I/O time? The norm usually reveals that I/O time just about doubles that of the processor.

Special nonstandard runs that exceed the set time limits for standard runs usually are run at night in a busy installation. In the case of often expected longer runs, it might be feasible to have a monitor with an automatic interrupt feature. With this system the computer can alternate between standard and special runs. Some time may be lost each time an interrupt is required, because appropriate storage of all



ADP OPERATING SCHEDULE — DATE:

	PRIME HOURS 0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	ETC.
CPU																
50K & BELOW							RJM				RJM	RJM			RJM	
100K & BELOW											SPR	SPR	RJM		SPR	
150K & BELOW											SPC-J	SPCC	SPC A		SPC G	
200K & BELOW				SPR			SPC-J									
201K & ABOVE	RJM	RJM	RJM	RJM	RJM	RJM		RJM	RJM	RJM				SPC-J		
TAPE UNITS																
(1)	X	X	X	X	X	X	X	X	X	SM	✓	✓	✓	✓	✓	
(2)	X	X	X	X	X	X	✓	X	X	SM	✓	✓	✓	✓	✓	
(3)	X	X	X	✓	X	X	✓	X	X	X	✓	✓	✓	✓	✓	
(4)	X	X	X	✓	X	X	✓	X	X	X	✓	✓	✓	✓	✓	
(5)	X	X	X	✓	X	X	✓	X	X	X	✓	✓	X	✓	X	
(6)	X	X	X	✓	X	X	✓	X	X	X	X	X	X	✓	X	
WK DISKS																
(1)	X	X	X	X	X	X	X	X	X	SM	✓	✓	X	✓	✓	
(2)	X	X	X	✓	X	X	✓	X	X	SM	✓	✓	✓	✓	✓	
(3)	X	SM	X	✓	X	X	✓	X	X	X	✓	✓	X	✓	✓	
(4)	X	SM	X	✓	X	X	✓	X	X	X	✓	X	✓	✓	✓	
READER	X	SM	X	X ✓	X	X	✓	X	X	X	X ✓	X ✓	X ✓	✓	✓	
PRINTER	X	X	X	X ✓	X	X	✓	X	X	X	X ✓	X ✓	X ✓	✓	✓	
PUNCH	X	SM	X	X	X	X	X	X	X	X	X ✓	X ✓	X ✓	✓	✓	
CMC 103	X	X	SPR	X	✓	X	✓	X	X	X				SPR	SPR	
TERMINALS	X															

CODE DEFINITION:
RJM = REGULAR JOB MIX DETERMINED BY SHIFT SUPERVISOR FOR BATCH AND TERMINAL JOB
SPC = ( ) SCHEDULED PROJECT BY JOB CLASS FOR DEVELOPMENT AND TESTING
SPR = SCHEDULED PRODUCTION RUNS
SM = SCHEDULED MAINTENANCE
X = BEING UTILIZED BY REGULAR JOB MIX
✓ = BEING UTILIZED BY OTHER THAN REGULAR MIX

Figure 1-3.—Typical daily operating schedule. 78.84

conditions within the main processor is required at the time of the interrupt. But this loss is normally insignificant compared to the improvement in the overall computer utilization.

Scheduling Operations

Scheduling operations cannot be a hit or miss proposition. Machine utilization at all times should be in accord with a predetermined schedule. The schedule should give the operating group either a specific listing of jobs to be done, or a specific timetable of the sequence in which jobs should be processed. Input data availability and all demands for machine time should be coordinated and reflected in the schedule. The schedule must make provision for regular production runs, special requests, program testing and assembly, unscheduled maintenance, and rerun time.

Scheduling can be considered as the act of screening all requests for machine time and allocating time on the basis of optimizing machine usage, meeting all prearranged commitments, reducing idle machine time,

minimizing personnel overtime, and designating sufficient time for contingencies.

There are several ways of establishing an effective schedule. Basically, the scheduling operation is spread out over a time period. Repetitive requirements may be planned as soon as they are known. For example, if a specific report is to be prepared on a specific date and the time requirement is two hours, this can be planned, because the requirement will remain static for as long as the job exists. Further, the approximate time of day can be specified according to the availability of input data or the need for output data.

A preliminary schedule should be devised on a monthly basis and should include recurring jobs. In developing this schedule, an examination of the following factors will provide enough information to outline operations throughout the month with some degree of accuracy:

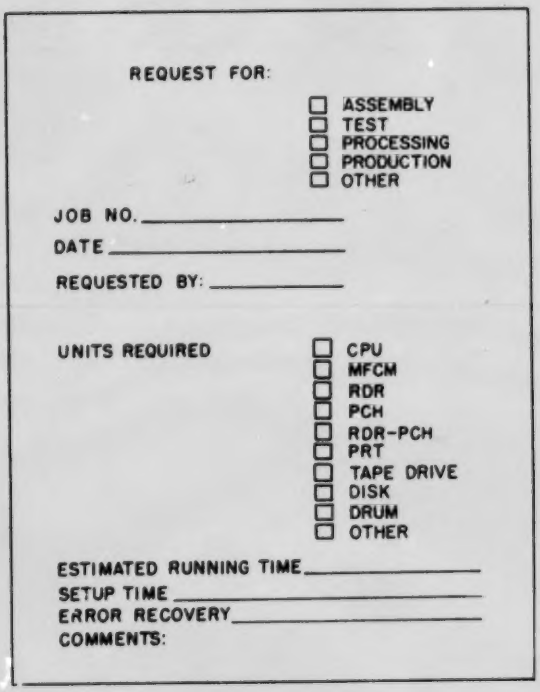
1. Is this a repetitive run or a one-time request? If it is repetitive, is it permanent or temporary?
2. Does the volume of data vary from one run to the next?
3. Does the production time take into account setup time?
4. Is the availability of the input data always on time or is it often late and incomplete?
5. Does the input data require extensive setup time?
6. Are there occurrences of poor data preparation or invalid controls?
7. What are the number and type of data errors and exceptions encountered?
8. What is the relationship of one application to another–can the setup functions be consolidated to facilitate setup time?

There are many things which will cause a variation in setup time. Examples include individual operators, the number of manual interventions required for a given program, and the mode of operation at the data processing center. Historical data that will aid in making reasonable estimates of setup time can be accumulated.

Estimates of program running time should be included with requests for machine time. The programmer can determine this estimate in the final stages of testing the program. An example of a machine time request form is shown in figure 1-4. Note that the entry "estimated running time" does not include setup time or provision for error recovery. These should be estimated by the scheduler and added to the programmer's time estimate.

The following questions should be answered for each installation before scheduling procedures can be established:

1. Who determines the priority and sequence of processing and issues schedule commitments?
2. To whom are requests for machine time made?
3. From whom do machine operators receive final machine schedules that indicate the actual job processing sequence?



78.76

Figure 1-4.–Job request.

The answers may differ greatly among installations, depending on the nature of the processing done, the size of the installation, the organization of management, and the extent of computer operation.

Several scheduling techniques may be applied during the scheduling period to determine the final sequence of processing. They are summarized below:

Priority System.–For many reasons, one program can take precedence over another. It may be determined, for example, that all the requests from the supply department will receive immediate attention, ahead of the requests from other departments. It may be that priority is dictated by the processing sequence of an application, or priority may have to be decided on the basis of a subjective evaluation.

Normal Frequency.–Regularly scheduled (that is, repetitive) jobs may take precedence over all others. In some cases repetitive work may not be required on a specific date and can be processed within a specified range of time.

Demand.–Jobs may be accepted and processed in strict chronological sequence, as requests for processing time are received.

Combination of the Above.–In most installations, actual scheduling is a combination of all of the preceeding techniques.

When scheduling machine time and when reviewing machine utilization, distinction must be made between different categories of time. This is of value for analysis, and for projections of machine requirements. If machine utilization analysis is done manually, forms used for scheduling machine time should have room for the actual time used to be posted after the fact. The Daily Log form, illustrated in figure 1-5, can be useful in this respect. However, the layout is not an important consideration as long as there is provision for the following categories of time:

1. Production time–time used for processing an application.
2. Assembly time–time used for program assembly or compilation.
3. Testing time–time used for program testing, whether used by operations or programming.
4. Training time–time used for training operation or programming personnel.
5. Preventive maintenance–regularly scheduled time when the machine is to be made available for maintenance.
6. Unscheduled maintenance or downtime–any time that computing equipment is under maintenance that has not been scheduled.
7. Rerun time–time required because of either operator error, data error, machine malfunction, or faulty input or output media. Whenever a job must be reprocessed, the reason should be indicated.
8. Buffer time–idle time allowed to give some schedule protection for unpredictable events during processing (example is a fire drill).

DAILY LOG

RUN NUMBER	DEPT	TIME											ERRORS		COMPONENTS USED							REMARKS
		ON	OFF	PRODUC-TION	ASSEMBLY	TEST-ING	TRAIN-ING	PM	DOWN	RERUN	BUFF-ER	OTHER	MACHINE	USER	CPU	RDR	PCH	PRT	MFCM	RDR-PCH	OTHER	

78.77

Figure 1-5.–Daily Log.

The amount of data and logging by hand should not be duplicated if the system software has automated logging capabilities.

Run Scheduling

Use of the run scheduling method permits estimating the completion time of any run, assuring the user when delivery can be met. For each individual operation, the setup time, start time, and completion time must be specified. Under this method it is necessary to develop a program for setting accurate time standards and an adequate internal communications system. For each job processed of the following minimum information is required:

1. The availability of input data
2. The volume or number of items handled or produced
3. The identification of the computer or work center assigned to do the operation
4. The time necessary to set up each required operation
5. The required running time for the job
6. The knowledge of the exact status of the run and its inputs and outputs as it relates to other runs

Scheduling by Shift

When shift scheduling, periods of time are allocated for various types of processing such as production, testing, compiling, and maintenance. Instead of attempting to do the detailed planning normally associated with run scheduling, each application is assigned to a specific shift or portion of the shift. No attempt is made to specify when, within the time period, the processing is to be started. At the beginning of each time period, each shift supervisor is provided a list of runs that must be completed during the period. It becomes the responsibility of the shift supervisor to determine the best sequence for doing the processing, or whatever. In short, the shift supervisor is responsible for the detailed scheduling within a shift.

PRODUCTION CONTROL AND SCHEDULING

In discussing scheduling, it becomes apparent that some of the production control functions are highly interrelated with scheduling computer operations. For instance, realistic scheduling is quite dependent on routing of work. Dispatching of work is dependent on planning and reporting. However, whatever technique is used, a good production control and scheduling system can reduce cost and be responsible to the user. Since computer time runs at a fixed rate of speed, the techniques to get the work done faster generally involve a new setup, scheduling, and handling techniques. A portion of the usable time of an ADP system is consumed by assembly, compiling, program checkout, sort, and other get-ready work to keep it running smoothly. It is this get-ready phase which offers a fertile area for cutting costs through better scheduling and handling.

USER SUPPORT

Support functions such as training seminars, user consultations, manuals, and regular center news bulletins are perhaps the most elusive user requirements to determine and evaluate. However, analysis of this type and frequency of user errors, use of existing vendor products, and user inquiries to support personnel usually provide the ADP technical manager with enough information to make intelligent and timely training and staffing decisions (figure 1-6). Additionally, the diligent logging and analysis of user problems and complaints may help to alleviate similar future problems.

RESOURCE MANAGEMENT

The most obvious responsibility of the ADP facility technical manager is the direct control of resources (equipment, space, personnel, etc.). The technical manager must continually balance resource costs against the requirements of the users. Having to work within an allocation budget, the ADP technical manager may find, over a time, that costs increase to the point that

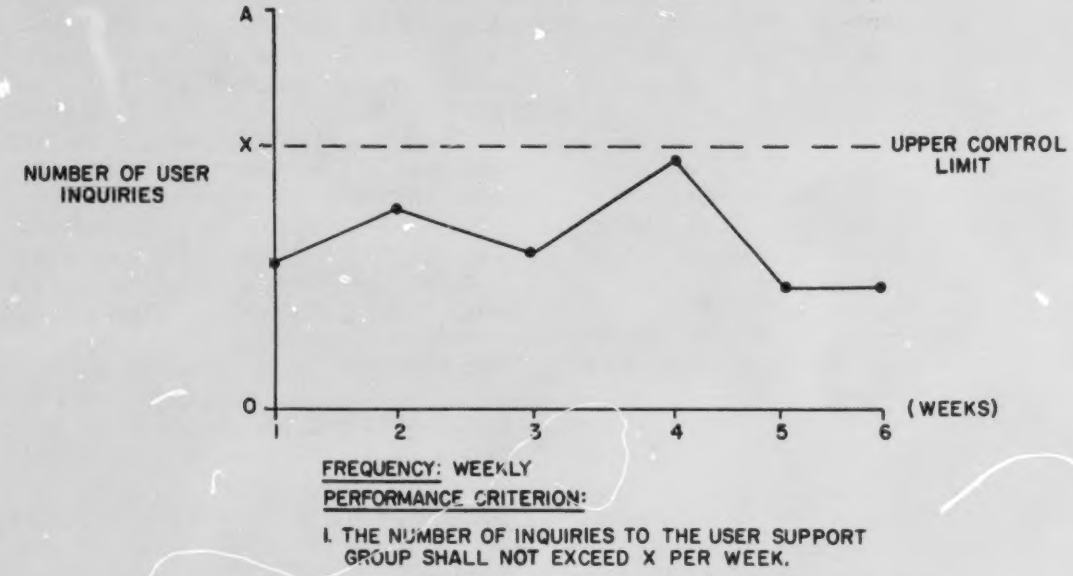


Figure 1-6.—Sample report for upper management on user support.

they exceed the command's allowable budget. This may be due to increased civil service personnel costs (ashore), decreased demand, inflationary increases in the cost of equipment and supplies, or procurement of additional hardware or software.

For ADP facilities with civil service employees, one solution to cutting cost is a cutback of civil service overtime. Elimination of underutilized peripheral equipment, elimination of unneeded operator shifts, and tight control of supplies are direct cost savings resulting from computer performance evaluation efforts.

Resource management also involves planning for the future. This implies that the ADP technical manager must have detailed information concerning the current workload—its history of growth, its present resource demands, its likely expansion in the future. The number of jobs completed per month, the percentage of utilization of major system resources, and the hours of system availability are several measures applicable to this problem. Performance data is thus valuable not only for enhancing the present system, but also for planning future resource requirements.

COMMUNICATING WITH UPPER MANAGEMENT

The ADP technical manger has a responsibility to report to upper management (civil service or military) on the status, performance, and requirements of the facility. The reports should include, at a minimum, summary information concerning the previously discussed areas of responsibility. The form of such reports is the responsibility of each parent command's upper management. This rate training manual can provide only general suggestions and nonauthoritative guidance as follows:

1. Status reports should be regular, concise, and preferably graphical in nature.
2. The amount of information reported should not exceed upper management requirements. "Too much, too often" is a problem common to many performance reporting schemes.
3. Information should be at a level of abstraction which upper management can easily

digest and understand, but sufficient to support the decision-making process.

4. The reports should compare the facility's current level of performance against a set of predefined performance goals.

Performance measures are thus not only a basis for satisfying the informational needs of the ADP technical manager, but also an effective means of communication between different levels of upper management responsibility within the command.

VENDOR RELATIONS

Although the increase in purchased ADP equipment has aroused considerable interest regarding ADP equipment maintenance, it is fundamental that whether the equipment is leased or purchased, the user must be assured of its reliable operation. Consequently, the data processing technical manager must devote special attention to scheduled and unscheduled maintenance to assure an uninterrupted flow of products to the user. Also, continued review of maintenance can avoid unnecessary data processing equipment costs.

The following common maintenance classifications and definitions are used:

CORRECTIVE MAINTENANCE (CM).– Maintenance performed by the technician (contractor or Government) which results from equipment failure and which is performed as required, and therefore, on an unscheduled basis.

PREVENTIVE MAINTENANCE (PM).– Maintenance performed by the technician (contractor or Government) which is designed to keep the equipment in proper operating condition and which is performed on a scheduled basis.

Close liaison with the vendor's local representative on maintenance matters is encouraged. The vendor is required, contractually, to keep the equipment in first-class operating condition. It is, therefore, mandatory that there is a complete understanding on all equipment maintenance matters between the ADP facility and the vendor's representative.

Local upper management must be thoroughly knowledgeable concerning all terms and conditions of pertinent contracts. In the maintenance areas, as in all others, these terms and conditions must be applied with care to ensure that the best interests of the Navy are served.

The Navy, in recent years, has expanded its potential to maintain ADP equipment with its own personnel, namely for that ADP equipment being employed aboard ships, remote locations, and security areas. When in-house maintenance capability is employed, the scope of the data processing technical manager's responsibility will increase.

Close coordination with assigned DSs is mandatory for proper maintenance. The technical manager's attention should also be focused on such items as stock levels, replenishment of peculiar parts through vendor distributors, and the host of problems associated with in-house supplies.

INSTITUTING A COMPUTER PERFORMANCE MANAGEMENT (CPM) PROGRAM

Although measurement and evaluation techniques are available to support the efficient and effective management of an ADP center, the question facing today's ADP technical manager is how to introduce this new technology into the facility. How often should the information obtained from performance data be reported to upper management, for example? In what form should it be reported? What is the ADP technical manager's role in instituting CPM procedures? The following paragraphs present a number of such issues that should be considered in inaugurating a performance management program.

CPM Reporting

Figure 1-7 depicts the life cycle of a typical computer system, progressing from an analysis of requirements to the final installation, operation, and enhancement of the selected system. In each phase of the computer life cycle, measurement and evaluation play major roles in satisfying the informational needs of the ADP technical and upper manager. As noted earlier, performance data is as useful during the requirements analysis phase as it is during the system enhancement phase. Every Navy ADP facility, regardless of size, should have some form of reporting during each phase of its system's life cycle. (See SECNAVINST 10462.18 series.)

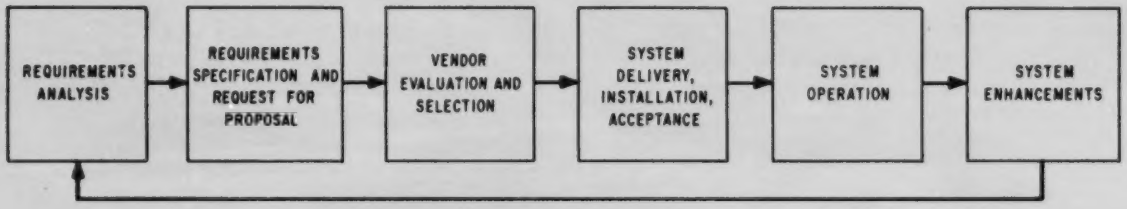
The types of data to be collected and reported should be determined not by their mere availability, but by the informational requirements of upper management. These informational requirements are in turn compiled by the ADP technical manager's scope of responsibility. Each report should provide a historical trend of the center's performance which is updated on a regular basis (depending upon the nature and importance of the information), and should contain specified performance criteria. These criteria may be translated into control limits on the performance charts. A control limit is a value chosen to represent the boundaries of acceptable performance for a given system variable. Some of these variables and their associated control limits may be "objective directed"—that is, they indicate the facility's ability to meet certain specified objectives (e.g., 1-hour average batch turnaround time). Others are "process directed," indicating the level of performance of internal system resources (e.g., the CPU, disks, or memory). When control limits are exceeded, an exception report is generated and, when appropriate, an in-depth study may be recommended to determine the specific cause(s) for the exception and appropriate remedies for correction.

Determining control limit values is highly dependent on the constraints and resources of the ADP facility, and indeed on the goals of the command. Frequently, past performance has been used as a standard against which current performance is evaluated. Although past performance does not necessarily mean good performance, it is a reliable indicator of the baseline system's natural reaction to various workload demands.

Finally, the performance reports generated by an ADP facility should always remain highly visible, especially to its user community. Publication of "performance charts" in the facility's regular newsletter is an excellent vehicle for accomplishing this.

EVALUATION AND IMPROVEMENT

An effective ADP installation involves the use of skilled data processing technicians and expensive, complex equipment. To employ these resources in an optimum manner demands continuing analysis of the operation. The establishment of good operating procedures and techniques does not necessarily mean that these methods will always be the best for continued operation. Changes in production requirements,



78.166

Figure 1-7.—The computer system life cycle.

workloads, and equipment necessitate continuous review of present procedures in an endeavor to obtain optimum results through a minimum of effort and cost.

Most Department of the Navy activities and contractor operations are required by SECNAVINST 10462.18 series to report on the equipment utilization and application. Although SECNAVINST 10462.18 series specifies the format for these reports, most activities require utilization data for their own use above and beyond what they are required to report.

The collection of operating data, analysis of utilization and performance, and continuous review of existing procedures are factors which can be used for evaluating the effectiveness of existing data processing systems and for improving the original plans.

When practical, results of the analysis can be presented in chart form displaying trends. These should illustrate to the technical manager the trend of the operations and point out areas which need detailed attention. Other results may be in report form for future guidance. Principal review areas of an installation's operations are:

1. Equipment utilization
2. Utilization rates
3. Benefits
4. Equipment capabilities
5. Manpower effectiveness
6. Maintenance
7. Production scheduling
8. Adherence to the installation's approved data processing program

MANAGEMENT'S ROLE

The ADP facility technical manager should play a central role in instituting and overseeing a CPM program. The scope and objectives of the program should be clearly established from the beginning so as to preclude any misconceptions and unnecessary data collection. Perhaps most importantly, subsequent control and review by the ADP technical manager is needed to guarantee that the program is continually meeting the organization's informational needs, in addition to ensuring that the morale of program personnel is maintained.

As an ADP technical manager, you should have a clear understanding and definition of the scope of your responsibilities and requirements from upper management. The objectives of any reporting program should be established and the information requirements should be defined in order to ensure that only pertinent data will be collected. The nature of the actual reports to be produced, the frequency with which they should be produced, and the performance criteria related to each should be determined. The reports should reflect enough, and ONLY enough, information for upper management to function effectively within the scope of their responsibility and higher authority requirements.

A successful CPM program requires skilled personnel who are intimately familiar with the computer resources being measured and the tools being used, and who have the ability to properly analyze and interpret the measurement data.

Any CPM program, or its equivalent type of program, should undergo a periodic review at least once a year. Changes in informational needs should be reflected in new CPM reports. Existing reports should be examined to determine their current relevancy. Too often at a Navy command, reports continue to be generated when there is no longer a need for them.

IMPROVEMENT THROUGH EVALUATION

The technical manager of an ADP installation should be on constant lookout for ways in which to improve the operating efficiency of the installation. Improvements may be made occasionally on the basis of sudden inspirations but, more likely than not, they are the result of a careful review and analysis of existing reports, procedures, machine usage, operation, and experience. Cooperation on the part of all personnel concerned, from upper management to data handlers, is essential if improvements most beneficial to an ADP facility are to be realized.

Improvement of Reports.—All reports being produced by a data processing installation should be reviewed at least annually to determine if the preparation of each report is justified, and if any changes can be made which will improve their quality. Increases in job requirements often result in the establishment of new reports, some of which may contain information similar to that in reports presently being prepared. It may be possible to consolidate two or more reports into one that will provide recipients with the required information, resulting in substantial savings of time and money within the ADP facility.

Improvement of Procedures.—Changes in report requirements may necessitate establishing new operating procedures or modifying existing procedures. New procedures which are put into effect without first analyzing existing procedures may overlap or duplicate work already being performed. On the other hand, cancellation of job requirements may eliminate some of the job steps in existing procedures. In the interest of realizing the most efficient operation, all operating procedures should be reviewed from time to time to determine whether any changes are required so that procedures may serve the most useful purpose.

Improvement of Machine Usage.—One of your principal objectives as a technical manager should be to achieve maximum utilization of the data processing equipment for which you are assigned control. Maximum value is assured only when such equipment is used productively to the maximum extent possible during a regularly scheduled work shift. A careful analysis of machine utilization over a period of time may reveal several important facts. It may reveal that certain machines are standing idle for several hours each day during the "slack period" but are used extensively for overtime work during a peak period. Machine rental rates generally are based on a stipulated charge for a specified number of hours of operational use time for each machine during a calendar month. Additional charges accrue when equipment is used in excess of the operational use time. In the interest of economy, the operating schedule should be analyzed and revised, if possible, to provide for more evenly distributed work throughout the rental period, thus reducing peak workloads and the amount of extra use charges.

In some cases an analysis of machine utilization may indicate consistent idle time for certain machines throughout the month. While this may be construed to mean that jobs are being performed in the most efficient manner, it means also that room for improvement still exists if maximum value is to be derived from the equipment. In this case, you should search for additional work which will produce results of value to the recipient without placing an undue workload on any given machine required for the job.

Improvement of Operation.—When productive tools are provided for performing jobs better and faster, there is a natural tendency to forget the job the PERSON is doing and to concentrate attention on the job the MACHINE is doing. While data processing equipment may perform many of the detailed, repetitive, and routine functions, the operator still performs important duties which the equipment cannot do. The operator must exercise the functions of control, analysis, judgment, decision, and evaluation, which remain the most important aspects of a given operation. Operation efficiency will vary, depending upon the training and experience of the operator and the nature of the job.

As equipment with greater productive potential is brought into use, the THINKING function of the operator increases in importance. To illustrate, consider the difference between an operation performed with an accounting machine and one performed with an electronic data processing system. If an operator using an accounting machine fails to set alteration switches correctly, a worthless report may be produced. When the error is discovered, the only corrective action necessary is to set the switches correctly and rerun the report. If an ADPS is being used, however, the operator may accidentally use master tape reels for a writing operation, and by inserting write rings destroy valuable records which may be extremely difficult or impossible to reconstruct.

Past performance records determine the standard operation efficiency which the technical manager uses when assigning time requirements to various jobs and when establishing schedules. It should be the objective of each technical manager to raise this standard gradually and continually. There are a number of ways in which the operating standards of data processing installation can be raised. A continuous on-the-job training program should be instituted and maintained for machine operators. Manuals of procedure containing accurate operating instructions for all jobs performed should always be available to operators. Morale should be kept high by promoting better working conditions, improving administrative relationships, and by being fair and impartial. Above all, a technical manager should exhibit those traits which mark an individual as being a real leader of people.

Use Idle Time Productively

Another method of improvement is to use idle machine time for productive pruposes. Some of this idle time may be used in relieving the peak workload period, as indicated previously. Other ways of reducing idle time include preparing additional reports in those areas not previously mechanized and adding more record-keeping functions to the machines when it is economical to do so. The economies that can result from mechanizing additional parts of the record-keeping activities of an organization can well justify the cost. When idle machine time is employed for additional work, the cost may be negligible compared with the results.

The use of idle machine time is more easily controlled for Electrical Accounting Machine (EAM) applications than it is for EDP systems. Sometimes it may be found that one facility cannot possibly find enough jobs to keep its hardware in full-time operation. In this case, the possibility of sharing the system with another organization should be investigated. (See SECNAVINST 10462.16 series; Subj: Government-Wide Automatic Data Processing Sharing Program.) In this way, maximum utilization of the system may be realized, while at the same time lowering the operating costs for the facility and providing services to additional users.

PERSONNEL EVALUATION

The efficiency of machine operators must be considered when assigning time factors to various jobs and establishing schedules for ADP operations. Likewise, the skill and experience of programmers must be considered when setting a target date for completion of a program. In either case, evaluation generally is based on a comparison of an individual's capabilities against standards established from past performances of skilled personnel.

When evaluating the work of a machine operator, it is important to consider training and experience. For a new operator the number of cards processed on EAM equipment or the number of errors made on a computer system are not so important as how much improvement is being made. This trend is the best indication of the type of production that can be expected in the development of each operator. The efficiency of an operator should be measured against established standards only after a level rate of production has been reached.

Skill and experience must be taken into consideration also when evaluating the efficiency of programmers. A new programmer may require an excessive amount of time and may encounter considerable difficulty during early attempts at writing programs. These programs may require extensive desk checking and machine testing before they can be executed successfully. Eventually, a programmer will have been writing programs long enough so that personal efficiency can be measured against expectations. A programmer who measures up to expectations may be considered qualified. On the other hand, it may be better to assign to other duties an operator who does not have what it takes to become a programmer.

PROGRAM MAINTENANCE EVALUTION

Program maintenance should be a matter of concern to everyone associated with it. Once a program is successfully converted to the data

processing system, it is subject to change. Experience has proven the need for and value of making periodic changes to a program after it is in operation. Some of the more common reasons for making program changes can be attributed to such things as:

1. Additional output needs
2. Desire for I/O format changes
3. Normal changes–such as new or obsolete requirements
4. Changes in ADP equipment, new or improved programming techniques, changes in auxiliary equipment, etc.
5. Changes in the scope of application
6. Realization that some aspects of a program's results are not acceptable
7. Unrealistic input requirements
8. Misunderstandings regarding the output requirements of the program
9. A possible or unforeseen condition or occurrence

Once a program is released for production, after final review, and found acceptable under operating conditions, it must be completely documented, as outlined in SECNAVINST 5233.1 series; Department of the Navy Automated Data System Documentation. This subject will be discussed in another chapter of this rate training manual.

Once these areas are covered, the original programmer should be relieved of most of the responsibilities of the program, and freed to work on another program. Since it is possible the original programmer may be transferred before a program is completed, all programs should be maintained by a predetermined section or division. Where major changes to a program are required, the original programmer, if available, may be called on for assistance.

The need for keeping documentation current is essential. Procedures must be established to ensure that changes made to programs are immediately and completely documented.

The section or division charged with program maintenance should maintain a master copy of each run manual. This master copy has a twofold purpose:

1. To prevent loss or destruction of program instructions
2. To facilitate the preparation of new run manuals in the machine room when they become dirty and/or torn

RESOURCE REVIEW AND REPORTS

For the proper guidance and requirements relevant to the management of automatic data processing resources and reporting, there are numerous higher authority instructions and standards to aid the DP1 or DPC (ADP technical manager) and upper management, at all levels of an ADP command. It is recommended that the following instructions and standards, with their references, be reviewed semiannually.

1. SECNAV INSTRUCTION 5200.28 series, Information Processing Standards for Computers (IPSC) Program. (This instruction will be reviewed briefly later in this chapter.)
2. SECNAV INSTRUCTION 5230.3 series, ADP users group program.
3. SECNAV INSTRUCTION 5231.1 series, Management of Automated Data System Development.
4. SECNAV INSTRUCTION 5238.1 series, Automatic Data Processing Program Reporting System (ADPRS)–Resources Accounting. (This instruction will be reviewed briefly later in this chapter.)
5. SECNAV INSTRUCTION 10462.16 series, Government-Wide Automatic Data Processing Sharing Program.
6. SECNAV INSTRUCTION 10462.18 series, Automatic Data Processing Review and Evaluation Program.

MANAGEMENT'S SOURCE MATERIAL

In addition to the various responsiblities and requirements demanded of a DP1 and above, an ADP technical manager must make sure that

proper publications, directives, instructions, and reference materials are available for the crew. The ADP technical manager's reference material should cover the parent command's ADPE. It should also cover all subjects pertaining to pay grade advancement for all enlisted personnel under the ADP technical manager's control.

A magnitude of subject area information is covered in the Federal Information Processing Standards (FIPS) publications. The use of these publications was approved by higher authority in SECNAV INSTRUCTION 5200.28 series, Information Processing Standards for Computers (IPSC) program. This instruction established the Information Processing Standards for Computers (IPSC) program for the Department of the Navy. It provides the framework for the development and implementation of ADP standards within the Department of the Navy and it provides the basis for formal Navy support for the international, national, federal, and DOD levels of ADP standards development.

The Department of the Navy IPSC program is an integral part of the Department of Defense IPSC program and is administered in accordance with procedures of Defense Standardization Manual 4120.3M. Included within the scope of the program are areas such as ADP terminology, problem description, programming languages, system documentation, automatic data processing equipment (ADPE) characteristics, input/output format and codes, source data media and fonts, and software.

The objectives of the IPSC program are to identify, develop, and establish those standards which will: (1) allow the integration of management information systems; (2) enhance information interchange through the use of standard or uniform data links and terms; (3) facilitate the development of machine independent computer systems; (4) make general use of related standardization efforts of ADP organizations; and (5) enhance the ability to interchange computer routines and programs among diverse ADP operating environments. Further, the program is to implement standards on a sustained, realistic timetable that anticipates and facilitates planned changes in equipment and related systems. The final objective is to avoid proliferation of premature standards which inhibit ADP and information systems' research and development efforts.

It is suggested that every ADP facility's ADP technical manager maintain a complete Federal Information Processing Standards register. The FIPS publication is a good daily reference and a ready reference to study for advancement in rate, as noted on the current advancement in rate bibliography, NAVEDTRA 10052-( ). The FIPS publications are used as a prime source of information to write advancement examinations from E-4 through E-7. The suggested secondary reading list to be studied before an advancement exam should contain, as a minimum, the following current issues of FIPS publications: 1, 2, 3-1, 7, 11-1, 14, 15, 20, 21-1, 22-1, 24, 25, 26, 30, 31, 35, 41, 42-1, 48, 49, 53, and 57. The following paragraphs give a brief synopsis of the recommended reading list of FIPS publications:

FIPS PUB 1: CODE FOR INFORMATION INTERCHANGE.–This document provides administrative, policy, and guidance information relative to the implementation and utilization of the standard code for information interchange. It is generally applicable to the representation of character-coded information in information interchange and files used in data processing, communications, and related equipments.

FIPS PUB 2: PERFORATED TAPE CODE FOR INFORMATION INTERCHANGE.–This document provides administrative, policy, and guidance information pertaining to the implementation and utilization of the standard perforated tape code for information interchange. It is generally applicable to the representation of character-coded information on perforated paper tape used with data processing, communications, and related equipments.

FIPS PUB 3-1: RECORDED MAGNETIC TAPE FOR INFORMATION INTERCHANGE (800 CPI, NRZI).–This document specifies the recorded characteristics of 9-track, one-half-inch-wide magnetic computer tape, including the data format for implementing the Federal Standard Code for Information Interchange at the recording density of 800 characters per inch (CPI).

FIPS PUB 7: IMPLEMENTATION OF THE CODE FOR INFORMATION INTERCHANGE AND RELATED MEDIA STANDARDS.–This FIPS publication provides further details covering the implementation of subjects covered in FIPS PUB 1, 2, and 3-1.

FIPS PUB 11-1: DICTIONARY FOR INFORMATION PROCESSING.–This document provides administrative, policy, and guidance information pertaining to the utilization of the American National Dictionary for Information Processing (X3/TR-1-77). This DICTIONARY is to be regarded as a guideline for general use throughout the Navy to help promote a common understanding of information processing activities. Its use is encouraged but is not mandatory.

FIPS PUB 14: HOLLERITH PUNCHED CARD CODE.–This standard specifies the representation of the Federal Standard Code for Information Interchange (FIPS 1) in 3 1/4-inch-wide, 12-row, rectangular-hole "Hollerith" punched cards, and is used in Federal information processing systems, communication systems, and associated equipments.

FIPS PUB 15: SUBSETS OF THE STANDARD CODE FOR INFORMATION INTERCHANGE.–This publication provides three subsets of 95, 64, and 16 graphic characters, derived from the Federal Standard Code for Information Interchange (FIPS PUB 1), which was adopted from the American Standard Code for Information Interchange (ANCII) (X3.4-1968). These subsets are used in Federal printers, display devices, punched card equipment, and other data processing or communication equipment which utilize a character subset less than the full 128 character set of FIPS PUB 1.

FIPS PUB 20: GUIDELINES FOR DESCRIBING INFORMATION INTERCHANGE FORMATS.–This FIPS publication provides guidelines which identify and describe the various characteristics of formatted information that should be considered whenever formatted information is interchanged. The objective is to clarify and improve the documentation necessary to effectively provide, process, or use the information involved. The guidelines provided are to be used throughout the Navy as a checklist for preparing effective documentation of formatted information interchange.

FIPS PUB 21-1: COBOL.–This FIPS publication announces the adoption of the American National Standard COBOL (X3.23-1974) as the Federal Standard COBOL. This ANSI publication defines the elements of the COBOL programming language and the rules for their use. The standard is used by implementors as the reference authority in developing compilers and by users for writing programs in COBOL. The primary purpose of the standard is to promote a high degree of interchangeability of programs for use on a variety of automatic data processing systems. The COBOL language is intended for use with business-oriented applications.

FIPS PUB 22-1: SYNCHRONOUS SIGNALING RATES BETWEEN DATA TERMINAL AND DATA COMMUNICATION EQUIPMENT.–This standard specifies the rates of transferring binary encoded information in synchronous serial or parallel form between data processing terminals and data communications equipments that employ voice band communication facilities.

FIPS PUB 24: FLOWCHART SYMBOLS AND THEIR USAGE IN INFORMATION PROCESSING.–This publication establishes standard flowchart symbols and specifies their use in the preparation of flowcharts in documenting information processing systems. This standard applies to any Navy information processing operation where symbolic representation is desirable to document the sequence of operations and the flow of data and paperwork.

FIPS PUB 25: RECORDED MAGNETIC TAPE FOR INFORMATION INTERCHANGE (1600 CPI, PHASE ENCODED).–This standard specifies the recorded characteristics of 9-track, 1/2-inch-wide magnetic computer tape, including the data format for implementing the

Federal Standard Code for Information Interchange at the recording density of 1600 characters per inch (CPI). It is one of a series of Federal Standards implementing the Federal Standard Code for Information Interchange (FIPS 1) on magnetic tape media.

FIPS PUB 26: ONE-INCH PERFORATED PAPER TAPE FOR INFORMATION INTERCHANGE.–This standard specifies the physical dimensions and tolerances of 1-inch-wide paper tape, including the size and location of the performations used for recording information.

FIPS PUB 30: SOFTWARE SUMMARY FOR DESCRIBING COMPUTER PROGRAMS AND AUTOMATED DATA SYSTEMS.–This publication provides a standard software summary form together with instructions for describing computer programs and/or automatic data systems for identification, reference, and dissemination purposes.

FIPS PUB 31: GUIDELINES FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT.–This publication provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. It treats security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off/site facilities, contingency plans, security awareness and security audit. It contains statistics and information relevant to the physical security of computer data and facilities, and references many applicable publications for a more exhaustive treatment of specific subjects.

FIPS PUB 35: CODE EXTENSION TECHNIQUES IN 7 OR 8 BITS.–This standard specifies methods of extending the 7-bit code of the ASCII (American Standard Code for Information Interchange) (FIPS 1), remaining in a 7-bit environment or increasing to an 8-bit environment, and builds upon the structure of ASCII to describe various means of extending the control and graphic sets of the code.

FIPS PUB 41: COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974.–The Privacy Act of 1974 imposes numerous requirements upon Federal agencies to prevent the misuse or compromise of data concerning individuals. This standard provides a handbook for use by Federal organizations in implementing any computer security safeguards which they must adopt in order to implement the Act. They describe risks and risk assessment, physical security measures, appropriate information management practices, and computer system/network security controls.

FIPS PUB 42-1: GUIDELINES FOR BENCHMARKING ADP SYSTEMS IN THE COMPETITIVE PROCUREMENT ENVIRONMENT.–These guidelines provide basic definitions and recommended practices to assist Federal agencies in organizing their benchmarking efforts.

FIPS PUB 48: GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION.–This guideline describes methods for verifying the identity of users seeking to gain access to computer systems or networks via terminals. Criteria are given for evaluating the effectiveness of personal identification techniques. System consideration for inclusion as further safeguards to data confidentiality are indicated, as a supplement to personal identification.

FIPS PUB 49: GUIDELINE ON COMPUTER PERFORMANCE MANAGEMENT: AN INTRODUCTION.–This guideline provides general assistance to Federal ADP managers in planning and organizing a Computer Performance Management (CPM) program.

FIPS PUB 53: TRANSMITTAL FORM FOR DESCRIBING COMPUTER MAGNETIC TAPE FILE PROPERTIES.–This publication provides a standard magnetic tape transmittal form (SF-277), together with instructions for providing the necessary information on the form. The standard magnetic tape transmittal form, Computer Magnetic Tape File Properties (SF-277), will be used by Federal agencies to document the physical properties and characteristics of a recorded magnetic tape file

needed by the receiving agency to process the tape.

FIPS PUB 57: GUIDELINES FOR THE MEASUREMENT OF INTERACTIVE COMPUTER SERVICE RESPONSE TIME AND TURNAROUND TIME.—These guidelines define measures and describe methodologies for measuring interactive computer network services.

FIPS ACQUISITION

In addition to the previously listed FIPS manuals, the ADP technical manager should acquire all publications, instructions, and directives listed on the DP's Bibliography sheet (NAVEDTRA 10052-( )). The American National Standard programming language FORTRAN manual (ANSI X3.9-1978) was adopted 15 November 1978 and was approved for voluntary use by the Departments of the Army, Navy, and Air Force. All FIPS and approved ANSI manuals can be ordered on DD Form 1425 from U.S. Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, Pennsylvania, 19120.

ADPPRS

Most ADP commands are required to submit certain reports to higher authority. One of these reporting procedures is covered in SECNAV INST 5238.1 series Department of the Navy (DON) Automated Data Processing Program Reporting System (ADPPRS). The senior DP in the command (the ADP DP technical manager) will probably be responsible for the submission of this report.

The ADPPRS is the DON system, implemented to collect data, that should be submitted to a Government-wide Automatic Data Processing Management Information System (ADP/MIS), administered and maintained by the General Services Administration (GSA). Data maintained in the ADP/MIS concerns the inventory and use of automatic data processing equipment (ADPE). The information obtained from the ADP/MIS is used to present appropriate information for the attention of ADP management, assist in negotiating improved terms and conditions for federal supply schedule contracts, records the ADPE acquisition history, isolates improper utilization practices, gauges sharing potentials, enhances reutilization possibilities, evaluates equipment purchase opportunities, and otherwise assists in the effective acquisition and management of ADPE and related resources.

Special government design (SGD) tactical ADPE and analog computers are fully exempt from the reporting requirements of the ADPPRS. SGD tactical ADPE is both integral to a combat weapon or space system, and is built

Control Fields	Data Submission Format Card Types			
	UA	SA	MA	D
UIC (Unit Identification Code)	X	X	X	X
CBC (Command/Bureau Code)	X			
SIN (System Identification No.)		X	X	X
Component Serial/ID No.			X	
Activity/Contractor Name	X			

Figure 1-8.—ADPPRS control fields and types of cards.

or modified to special government design specifications. An analog computer is a computer which represents variables by physical analogies. In general, an analog computer uses an analog for each variable and produces analogs as outputs, whereas a digital computer counts descretely.

ADPPRS data is to be reported in accordance with SECNAVINST 5238.1 series to COMNAVDAC, code 91. There are four categories of data submission format cards. The four categories are (1) ADP Unit Identification, card type is UA; (2) ADPE System Inventory, card type is SA; (3) ADPE Component Inventory, card type is MA; and (4) ADPE System Utilization, card type is D. Figure 1-8 shows a matrix of control fields and types of ADPPRS cards with the data elements required for each data submission transaction. Certain data elements (control fields), shown in figure 1-8, are common across all aggregations of data and for all data submission formats prescribed for ADPPRS in SECNAVINST 5238.1 series.

Every DP1 and above should review SECNAVINST 5238.1 series on a semiannual basis. The material and reporting procedures contained in this instruction are too voluminous to include in this chapter but will be used in rate advancement examinations.

CHAPTER 2

ADP ORGANIZATION AND PERSONNEL

The organizational structure of the Navy's automatic data processing community has gone through many significant changes since 1977. As a DPI or DPC, you should know management strategies, e.g., methods of personnel acquisition, the delineation of personnel responsibilities, and the organizational structure of an ADP organization. These and other major areas of concern are presented in this chapter as information/guidelines only. The suggestions contained in this chapter are not the only means of organizing an ADP installation.

PERSONNEL ADMINISTRATION

Personnel administration is the management of people. The administration of naval personnel involves recruitment, classification, training and development, assignment and rotation, transportation, discipline, advancement, personnel records, personnel accounting, performance evaluation, separations, and retirement, as well as providing morale services.

RESPONSIBILITIES

The objectives of personnel administration in any organization are (a) to supply the organization with a number of people sufficient to man the billets or work stations of that organization, (b) to effect the best possible distribution of people throughout the organization, and (c) to ensure maximum utilization of personnel. Manpower management determines personnel requirements and ensures the effective use of available manpower. Concepts of personnel administration and manpower management are equally applicable to the Navy, business corporations, educational systems, and research organizations.

Naval manpower management and personnel administration are engineered to cope with personnel problems inherent at all organization levels. Additionally, it must cope with special problems posed by the size of the Navy, the variety of its functions, the global scope of its operations, the mobility of its forces, the rate of change and complexity of its technology, the turnover and rotation of its personnel, and the requirement to develop and implement its own training programs.

To cope with these formidable problems, the Navy utilizes personnel specialist to aid in the planning and implementation of procedures and actions. These specialists and others who have responsibilities and duties connected with manpower management and personnel administration are, in turn, supported by a modern data gathering, processing, and reporting system which provides timely and accurate information necessary to make decisions.

Responsibility for manpower management in the Navy begins with the Secretary of the Navy, who has an Assistant Secretary for Manpower and Reserve.

MANPOWER MANAGEMENT

Manpower management includes planning, statistical forecasting, balancing, and approving manpower requirements. These requirements relate to the specific numbers and kinds of military billets required by each activity (sea or shore) to perform its assigned mission and tasks.

Billet and shore position requirements must at all times adequately provide for operational readiness, augmentation of the fleets, maintenance, administration, training, and sea/shore rotation. Planning and control of manpower and the effective utilization of manpower to meet such requirements are proper functions of management (command) coordination.

CHIEF OF NAVAL OPERATIONS

Management of Navy military manpower is a responsibility of the Chief of Naval Operations, who has a Deputy Chief of Naval Operations for Manpower and Naval Reserve. The officer assigned to this billet is also the Chief of Naval Personnel, which illustrates the close relationship between manpower management and personnel administration. (Marine Corps manpower management is a responsibility of the Commandant of the Marine Corps.) Military manpower management is a function of command and operates through the military chain of command.

The manpower requirements resulting from the systems and subsystems described in OPNAV Instruction 1000.16 (series) provide the base from which plans are developed to procure, train, and assign personnel. The Chief of Naval Operations directs and coordinates the development and implementation of the manpower planning system with the following objectives:

1. To determine minimum military and civilian manpower requirements to achieve approved operational and mission demands

2. To provide staffing standards for functions performed ashore and afloat, based on recognized management and industrial engineering techniques and objective determinations of workload

3. To provide a system for the aggregation of manpower requirements information at the various levels above the activity level

4. To support and justify Navy manpower requirements during all stages of the Planning, Programming, and Budgeting System

5. To relate support manpower requirements within the shore establishment to the changing demands of the operating forces

6. To minimize response time for manpower information by responding rapidly to management queries

7. To ensure that manpower requirements for the maintenance and operation of new weapons, equipment, systems, and initiatives are known far enough in advance of fleet introduction to allow their consideration in the programming cycle and to allow the development of requisite personnel skill levels and

8. To provide reliable planning information to personnel inventory managers, both military and civilian, so they may assess the feasibility and impact of manpower management actions.

MANPOWER SUPPORTING ORGANIZATIONS

While policy control and direction of the Navy Manpower Requirement System is vested in the Chief of Naval Operations, important support for these programs is provided by two major field components, the Navy Manpower and Material Analysis Centers, Atlantic and Pacific (NAVMMACLANT/NAVMMACPAC). The purpose of these commands is to apply work study and management engineering techniques throughout the Naval Establishment in order to document and recommend (by means of onsite surveys, special studies, and evaluation of material maintenance support), the optimum use of manpower and material resources in carrying out assigned missions. Additional responsibilities include stocking and maintaining manpower listings for the Naval Establishment; storing and issuing all promulgated manpower documents; operating the Naval School of Work Study; and performing such other manpower or material analyses and work study functions as may be directed by the Chief of Naval Operations.

HOW MILITARY MANPOWER IS ACQUIRED

The senior DP may be required to participate in planning the DP allowance when

ordered to a "new construction" billet or assigned to a command acquiring an additional or larger computer system. It is also probable that the current allowance is ineffective and requires adjustment to meet the command's present ADP requirements. Requesting new or additional allowances requires a knowledge of all the skills that are required in a computer installation. The following paragraphs provide an overview of the events related to establishing manpower requirements and should be valuable to the senior DP involved in allowance planning.

Military manpower requirements are included in the Department of Defense Planning, Programming, and Budgeting System. This system operates on an 18-month cycle and is repeated annually. Events in this cycle which are necessary for the development and authorization of Navy military manpower requirements are briefly summarized in the following paragraphs. This information is provided to enhance the understanding of how manpower is acquired.

Intelligence is collected and an appraisal is made of any potential threat to the security of the nation. The President, the National Security Council, and the Department of Defense are involved in these actions.

Based upon national policy, a strategy is developed to meet any threat to national security. This strategy is developed by the Joint Chiefs of Staff (JCS) and submitted to the Secretary of Defense.

The Secretary of Defense issues the Defense Policy and Planning Guidance, and also the Material Support Guidance (draft Logistics Guidance).

Based upon the planned strategy and the Secretary of Defense Guidance, the Joint Chiefs of Staff identify requirements and objective forces necessary to meet the threat under the policy guidance. These requirements and objective forces are not fiscally constrained in these planning actions.

The Secretary of Defense then issues to the JCS a Planning and Programming Guidance Memorandum; Fiscal Guidance and Material Support Planning Guidance; and Guidance for Program Objective Memoranda/Joint Force Memorandum Preparation.

The JCS submits to the Secretary of Defense a Joint Force Memorandum. This memorandum contains recommendations for forces and resources, rationale and risk assessments. These recommendations are fiscally constrained to conform to the Fiscal Guidance previously issued by the Secretary of Defense.

Based upon the JCS Joint Force Memorandum, the military departments, and defense agencies develop and submit program objectives memoranda (POM) to the Secretary of Defense. Each POM contains forces and resource recommendations with rationale and risk assessment. The POM is fiscally constrained to conform with the Fiscal Guidance previously issued by the Secretary of Defense. The POM is developed by fiscal year, and is concentrated two fiscal years in advance of the current fiscal year. It includes planned projections of forces programmed for eight fiscal years and manpower programmed for five fiscal years. It is emphasized that the required forces are first determined, then manpower requirements necessary to support the planned forces are determined. Therefore, manpower requirements are first introduced into the system during the development of the POM. The Department of the Navy's POM is the Secretary of the Navy's annual recommendation to the Secretary of Defense for the detailed application of Department of the Navy resources.

Upon receipt and analysis of each military department's POM, the Secretary of Defense issues program decisions. These decisions include intended adjustments in the POM submissions. Rebuttals to these decisions may be submitted by the military departments; then final program decisions are issued.

When program decisions are finalized, departments/agencies submit to the SECDEF budget estimates for the budget year. The budget year is usually the fiscal year in advance of the current fiscal year and is the first program year of the Five-year Defense Plan (FYDP).

Upon receipt and evaluation of the budget estimates, the SECDEF issues program budget decisions and submits the Department of Defense budget as part of the President's budget submitted to Congress.

MANPOWER AUTHORIZATIONS

The manpower authorizations (OPNAV Form 1000/2) promulgated by the Chief of Naval Operations are the detailed expression of the numbers (quantity) and types (quality) of the Navy military manpower authorized for each Navy activity.

As an integral part of the Navy's manpower, personnel and training information system (MAPTIS), the manpower authorization has the following uses and applications:

1. As an expression of the manpower needs of an activity, it is the authority used by the Commander, Naval Military Personnel Command and the applicable enlisted personnel distribution office to provide requisite personnel distribution and Naval Reserve recall.
2. It is the basic document for current and future peacetime and mobilization Navy military manpower planning in the areas of recruiting, training, promotion, personnel distribution, and Naval Reserve recall.
3. It is the single official statement of organizational manning and billets authorized.

All Navy manpower authorizations collectively reflect the total Navy military manpower apportionment resources as authorized by the Secretary of Defense in the Department of Defense Five-year Defense Program (FYDP). The total Navy-wide mobilization military manpower is phased from the day of mobilization through the succeeding 12 months. Total Navy-wide manpower authorizations cannot exceed the end-strength authorized by the Secretary of Defense for each fiscal year. Mobilization requirements, however, are not subject to end-strength limitations.

The Navy's annual program objectives memorandum (POM) is the primary vehicle for proposing FYDP manpower adjustments to the Secretary of Defense. Accordingly, any uncompensated request for manpower increases should be included in the POM. Once the POM for a particular fiscal year has been reviewed by the Secretary of Defense and Program Decision Memorandum (PDM) issued, no further increases to a program are usually possible except by reprogramming within existing resources. Accordingly, changes to an activity's mission, tasks, or functions, which will require manpower changes, must be identified to the Chief of Naval Operations a minimum of 18 months prior to the beginning of the fiscal year in which the manpower change is required. This early notification is essential if the desired manpower change is to be included in the POM.

REQUESTING CHANGES TO MANPOWER AUTHORIZATIONS

Changes to OPNAV Form 1000/2 often involve a change to the billets authorized for an activity, necessitating the movement of personnel to fill the revised authorization. Frequent and numerous billet changes result in excessive administrative efforts in the management of Navy military manpower and an unnecessary expenditure of severely limited financial resources.

Early identification of billet changes which will require the movement of personnel is essential if the required personnel are to be onboard when needed. In order to allow sufficient time for orderly personnel detailing, any changes which require permanent change of station (PCS) orders to a geographical area are projected with an effective date at least four months from the date of approval.

Administrative Chain of Command

When requests for changes are forwarded which include quantity, grade, or rate increases, but do not identify compensation, the chain of command makes recommendations regarding compensation. The Chief of Naval Operations retains decision authority on all change requests.

Commanding Officers.—Individual commanding officers are responsible for keeping their manpower claimants informed regarding the manpower situation and for ensuring that the number of billets (including skills, paygrades, and special qualifications reflected in manpower authorizations) are the minimum military requirements necessary to support the

mission, tasks, and functions of the command. In order to ensure optimum manpower utilization, each commanding officer should periodically review and evaluate manpower authorizations, including mobilization requirements, and, when appropriate, recommend changes to the manpower claimant via the chain of command. Particular emphasis should be placed on identifying areas in which manpower may be saved and/or skill levels reduced without adverse effect on mission accomplishment. The probability is extremely low for the approval of increases for which compensatory decreases are not identified. The following checks should be applied to change requests:

1. Change requests are to be submitted a minimum of 10 months prior to the effective date of the desired change.
2. Each requested action is to be complete and accurate and is to include necessary mobilization requirements.
3. A complete justification is to be provided in each request for a revision.

If it becomes necessary to request increases without complete compensation from within the manpower assets of the activity, a priority for each of the requested billets should be indicated to assist the manpower claimant in making recommendations to the Chief of Naval Operations. Should the identified compensation be insufficient, invalid, or unacceptable, approval of only portions of the request may be possible.

As appropriate, change requests should be initiated to establish new component activities and required billet transfers when detachments are established at locations geographically separated from the parent activity. Requested changes should be summarized by designator/grade or rate/ratings.

Manpower Claimants.–The manpower claimant is the command, bureau, or office in the administrative chain of command assigned the responsibility by the Chief of Naval Operations for management of manpower requirements of assigned activities. Requests for changes in manpower authorizations are forwarded via the chain of command to the manpower claimant. The manpower claimant will then forward requests that are recommended for approval to the Chief of Naval Operations. Following are some of the specific responsibilities of the manpower claimant:

1. To perform final review of all change requests forwarded through the chain of command and forward those requests recommended for approval to the Chief of Naval Operations with appropriate recommendations, including comments concerning the applicability and availability of compensation.

2. To ensure that information copies of those change requests recommended for approval are forwarded promptly to appropriate program element sponsors with copies of all endorsements.

3. To respond promptly to requests from the Chief of Naval Operations for specific activity changes required to implement manpower end-strength adjustments directed by higher authority.

4. As necessary, to coordinate with other manpower claimants when proposed changes which affect activities under the command of one manpower claimant have significant impact on the operational capabilities of activities under the command of another manpower claimant.

5. When proposing changes in mission, tasks, or functions of an activity, to ascertain the manpower implications of the proposed change. This includes the requirement to arrange for associated programming of manpower, quantitatively and qualitatively, in phase with the change.

6. To recommend to the Chief of Naval Operations billet requirements for assigned activities and planned mobilization activities which do not exist in peacetime.

7. To establish internal manpower analysis and validation procedures to accomplish a review of the mobilization manpower allocation/requirement plan (M-MARP) which is promulgated, annually, by the Chief of Naval Operations.

8. Upon completion of the annual review of the M-MARP, to submit Manpower Authorization Requests (OPNAV Form 1000/4A) to the Chief of Naval Operations

(Op-01BG). The revision should reflect all changes which are required to be made to activity manpower authorizations.

9. As necessary, to assume the responsibilities of commanding officers for planned activities not currently in existence.

ORIGINATING CHANGES

Requests for changes will be submitted on the Manpower Authorization Request (OPNAV Form 1000/4A), except for the short format for requesting minor changes. The completed form is forwarded under a letter which must reference the transaction number and date of the manpower authorization on which the requested change is based and must include the justification for the requested change.

Bold, legible hand printing is acceptable on any OPNAV Form 1000/4A submission. The expense of typing these forms is seldom warranted. The expense of photographically reducing these forms is never warranted, since reduced forms cannot be used because a new manpower authorization can be generated only with a keypunch operation that uses completed full-size OPNAV Forms 1000/4A.

Officer and Enlisted Billet Changes

Separate OPNAV Forms 1000/4A must be prepared in requesting changes to officer and enlisted manpower authorizations. When either the officer or enlisted change request is prepared, consideration must be given to all officer or all enlisted billets in the activity that will be affected by the change. This consideration includes billets which result from projected change to the MARP code or activity code.

However, unless a complete reorganization is being requested, only those billets to be added, changed, or deleted are entered on OPNAV Form 1000/4A. The original and two copies of the form are submitted to the CNO; additional copies should be prepared as required for retention by the originator and intermediate addressees.

New OPNAV Form 1000/2

Approval or partial approval of a change request will result in preparation and distribution of a new manpower authorization, OPNAV Form 1000/2, if significant changes are made. However, minor changes in most cases do not justify the cost of printing and distribution. In these cases, most of the data reflected in the billets authorized may be verified by checking the officer data control report (ODCR) for officer billets and the Enlisted Distribution Verification Report (EDVR) for enlisted billets. The transaction number on each of these reports should be noted and compared with the transaction number on the activity's latest manpower authorization. If the number is different, then there is probably a minor change that has been approved which did not warrant reprinting a new manpower authorization.

Short Format For Requesting Minor Changes

A short format for requesting minor changes to manpower authorizations is authorized to reduce response time. The use of this format is restricted to minor changes not requiring quantitative or qualitative compensation. Only requests for changes in Navy enlisted classification code (NECs) incident to changes in shipboard equipment, billet title changes, and correction of errors noted in manpower authorizations should be submitted using the short form. It is not to be used for requesting additional billets or changes to paygrades.

The format (fig. 2-1) is adaptable for use in official correspondence and messages but is intended for use primarily in speedletter format.

The request should be brief and concise, and should present specific substantiating data which includes equipment identification for NEC revisions.

The short format may be used only by fleet and fleet staff units. When the originator of a request believes that the Chief of Naval Operations can act upon the request without comment or recommendation by officers in the chain of command, the request may be sent directly to the Chief of Naval Operations.

(Classification)
(Originator)
(Date)

Manpower Authorization (Activity Title), Transaction Number _____ of (Date) _____.

Situation: Describe changed requirements necessitating revision of the manpower authorization. Include authority for, or cause of the changed requirements. This paragraph constitutes the justification for the request.

Billets: Identify billets by Billet Sequence Code, title (if any), designator or rating, grade and whether base or augment. Indicate recommended changes on a separate line.

Specific Action Recommended: Include the estimated time to implement if immediate action is not required.

Copy to:
Administrative chain of command
Program Element Sponsor

Figure 2-1.–Manpower Authorization Short-Format Change Request.

However, copies are sent to the administrative chain of command and to the program element sponsor.

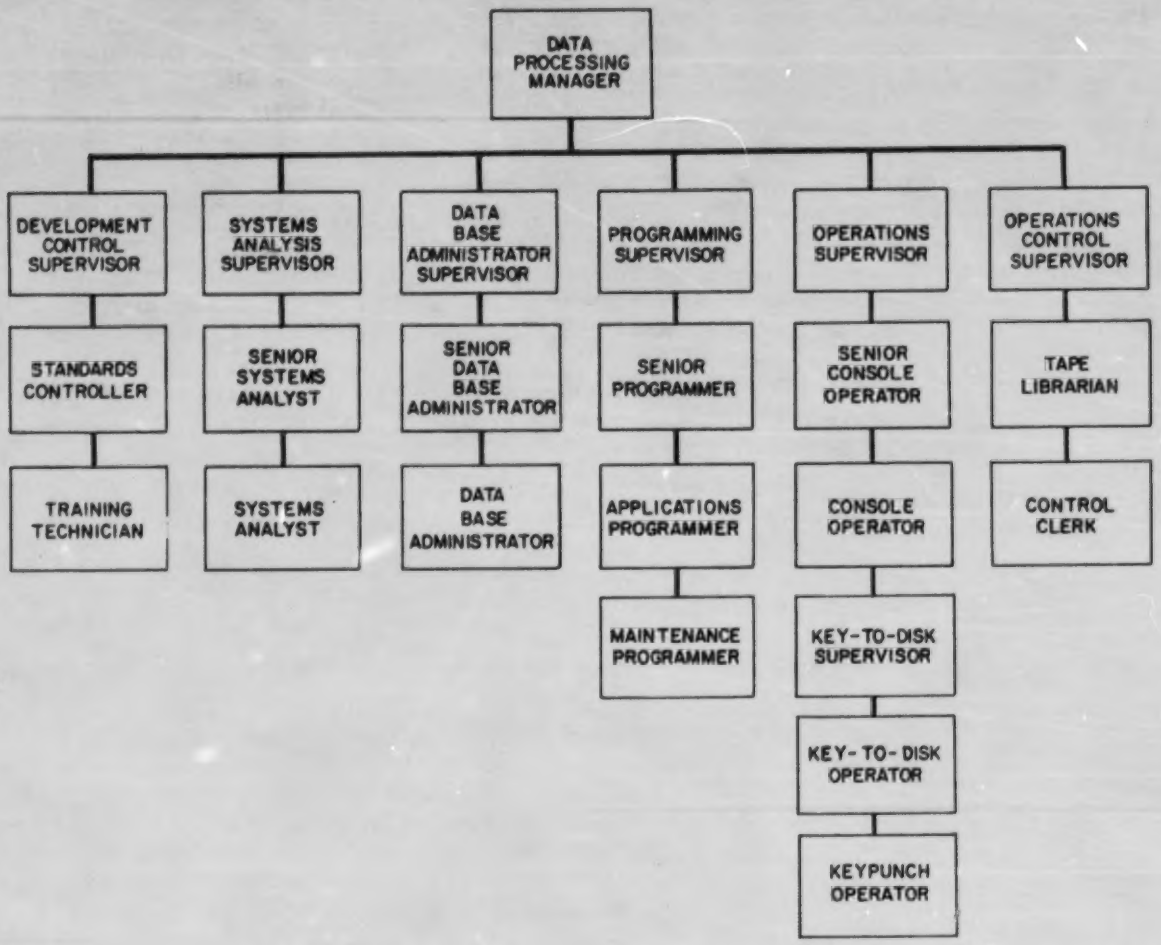
If additional information should be required to clarify a requested change, the originator or appropriate official in the chain of command will be informed of the specific information desired.

PERSONNEL REQUIREMENTS

The senior DP at an ADP installation is usually required to identify skill requirements to satisfy the appropriate billet structure allowance. It is, therefore, important to have a thorough knowledge of the various tasks and skills that are needed at an ADP installation. The Navy assigns billets mostly by NECs. The NECs available do not, however, truly reflect in their descriptions the many diversified positions that could be required in a large ADP organization. The various DP positions must first be defined. The descriptions of the available NECs can then be screened, and those best filling the various positions at an ADP facility can be selected.

As a general guide, figure 2-2 will help identify the various positions in a large ADP organization. These positions are described in the following paragraphs. The total number of personnel required for each billet description depends upon the mission of the ADP facility, the required workload, and the required hours of operation. These factors vary from one ADP facility to another. The responsibilities and duties for the following billet descriptions are discussed throughout this rate training manual and the *DP 3 & 2* manual (NAVEDTRA 10264-D).

DATA PROCESSING MANAGER–The incumbent is the administrative and technical head of all data processing activities for a particular ADP facility. The individual in this billet is responsible for all data processing



78.148

Figure 2-2.—Billets Within a Large ADP Organization.

performed by the facility, including systems analysis, administration, programming, and operations. This individual serves as liaison to authorized users of data processing services and develops improved techniques and methods for assisting a command's mission.

STANDARDS CONTROLLER—This individual coordinates data processing standards development and implementation; enforces methods and performance standards; audits adherence to the prescribed standards; and reports deficiencies to the supervisor of development control.

TRAINING TECHNICIAN—This individual organizes, schedules, and coordinates all data processing training activities, including:

1. Departmental instruction for new personnel
2. Programmer and operator training
3. Professional technical development
4. Management and supervisory training

SYSTEMS ANALYSIS SUPERVISOR—This person provides technical analytical assistance in identifying and solving the system's problems, deals with personnel throughout the command,

and is required to coordinate project control and approval.

SENIOR SYSTEMS ANALYST–This individual is assigned to systems projects to provide direction and control within the specifications of the project schedule. As project leader, the senior systems analyst participates in the project organization and scheduling and is in direct liaison with the management and personnel of the user department. The position carries project (but not administrative) responsibility over the systems analysts assigned. The incumbent fulfills the detailed duties of the systems analyst, as required.

SYSTEMS ANALYST–Under the direction of a senior systems analyst, the systems analyst participates in the analysis of systems problems and the development of problem solutions concerning hardware and software. This individual is responsible for working with personnel in problem areas and defining the pertinent specifications of information requirements and operational needs. The systems analyst must make formal presentations, conduct interviews, and submit written reports for review purposes.

DATA BASE ADMINISTRATOR SUPERVISOR–This person is assigned as central manager of all data bases. The incumbent manages, controls, and directs the organizing of the data base management system and data base schemas. The DBA supervisor approves all software and hardware changes affecting structure and administrative handling of the data base.

SENIOR DATA BASE ADMINISTRATOR–This individual is assigned as systems technician to provide direction and control within command specifications for Data Base Management Systems (DBMS) and inherent schemas. As senior technician, the incumbent is in direct liaison with systems, programming, and user departments for all local data bases.

DATA BASE ADMINISTRATOR–Under the direction of the senior DBA, the incumbent is assigned as the ADP facility DBA in planning, designing, developing, implementing, testing, documenting, and maintaining the entire data base environment. The DBA coordinates all data base activities between management, analysts, programmers, operators, and users. The DBA maintains and updates DED/D, the DBMS schemas, and the other data base support software.

PROGRAMMING SUPERVISOR–The programming supervisor provides technical and administrative direction to the development of new programs and maintenance of operational programs. In this capacity, the programming supervisor is in direct liaison with systems personnel, operations personnel, and representatives of user departments.

SENIOR PROGRAMMER–This individual is assigned to programming projects to provide direction and control within the specifications of the project schedule. As senior programmer on the project, this person participates in project organization and scheduling and is in direct liaison with the systems analysis project leader. This position carries project (but not administrative) responsibility over the programming personnel assigned. As required, the incumbent fulfills the duties of a programmer.

APPLICATIONS PROGRAMMER–Under the direction of a senior programmer, the applications programmer participates in analysis liaison with a systems analyst, and creates program logic structure and codes. Other programming tasks include producing reports and mathematical computations, and maintaining information files. This individual prepares the required logical interface between related programs, and assists, as required, in the solution of operation difficulties encountered in existing programs.

MAINTENANCE PROGRAMMER–Under the direction of a senior programmer, the maintenance programmer takes action to improve program performance or to correct deficiencies. This person also performs all programming tasks needed to implement the

changes, including testing and updating of program documentation.

OPERATIONS SUPERVISOR–This individual supervises the operation of all digital computing equipment, key-to-tape/disk equipment, keypunching and verifying machines, and other media conversion devices. In this capacity, the operations supervisor reviews equipment and personnel performance, and develops techniques to improve performance. The incumbent reviews new applications and programs, and projects their effects on equipment operation for management evaluation.

SENIOR CONSOLE OPERATOR–The incumbent operates and controls digital computing equipment by means of a peripheral console device or auxiliary control panel. The senior console operator prepares the computer for program processing and is responsible for the satisfactory completion of each scheduled computer operation.

CONSOLE OPERATOR–This individual operates digital computing equipment with a console device or auxiliary control panel. Under the direction of the senior console operator, the console operator prepares the computer for program processing and operates the equipment for the completion of a scheduled program.

KEY-TO-TAPE/DISK SUPERVISOR–The incumbent supervises the operation of the system computer with associated equipment, including the keystations, magnetic disk unit, magnetic tape unit, teleprinter, and supervisory console which houses the system's computer. This individual also manages and supervises the preparation of source data entry.

KEY-TO-TAPE/DISK OPERATOR–Under the direction of the key-to-tape/disk supervisor, the key-to-tape/disk operator controls computer equipment by means of a supervisory console; prepares source data entry material for keying and processing; and displays data on video screens for immediate verification and correction.

KEYPUNCH OPERATOR–The keypunch operator keypunches/keyverifies data as directed by the keypunch supervisor or the supervisor.

OPERATIONS CONTROL SUPERVISOR–This individual directs the control and coordination of all operational facilities through supervising library activities, production control procedures, and operating standards. This person is also concerned with developing and enforcing procedures, and in several instances, with supervising the personnel who execute the procedures.

TAPE LIBRARIAN–The tape librarian stores and circulates program documentation, and controls foreign tapes and data maintained on all recording media. This person performs a multitude of administrative duties, such as filling out tape labels, run requests, degaussing control forms, and security check lists.

All of the previously described positions or any that may be desired at an installation must be designated by an NEC. A complete roster of Occupational Standards, which covers a thorough list of duties for all DPs, can be found in the *Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards* (NAVPERS 18068-D).

ADP INSTALLATIONS

Smaller ADP installations are not allowed the luxury of having specialized people for each specialized position. However, these smaller installations (such as most ships) do have other advantages over the larger ADP installations ashore. The most evident advantage is that a DP aboard a ship is involved with all aspects of the data processing field. A DP aboard ship could be expected to function in billets ranging from the senior systems analyst to a keypunch operator.

The cross-training a DP receives aboard ship is very beneficial, allowing this person to become a completely trained data processor. The close working relations with the departments and divisions requesting data processing services will help the DP aboard ship become qualified in more occupational standards before a DP ashore. This allows for complete familiarity with a system and provides an invaluable background for future Navy duty assignments and advancement opportunities.

No. of Computers	Total Memory		Total Purchase Price*	Size
	Words (W)	Bytes (B)		
1	greater than or equal to 100K	greater than or equal to 400K	greater than or equal to $1.5M	Large
	greater than or equal to 10K	greater than or equal to 30K	greater than $500K	Medium
2-5	greater than or equal to 600K	greater than or equal to 3.2M	greater than $8.0M	Large
	greater than or equal to 60K	greater than or equal to 180K	greater than or equal to $3.0M	Medium
Any number	Any amount		greater than $16.0M	Large
			greater than or equal to $8.0M	Medium
Anything else	Anything else		Anything else	Small

*If equipment is rented, purchase price equals monthly rental multiplied by 40.

Source: Naval Audit Service

Figure 2-3.–Table for Computing DPID Size.

A senior DP can compute the size–small to large–of a particular ADP activity's automatic data processing installation department (DPID) utilizing the chart in figure 2-3. The size is based on total memory size and total purchase price of an activity's computer(s). For an activity to have a DPID, it must have at least one central processing unit (CPU) and one computer operator.

For an activity to have a data processing programming support department (DPPSD), it must have an organizational element whose primary function is to design, develop, or maintain application software/computer programs. An ADP activity with fewer than five programmers/analysts/specialists is not usually considered to have a DPPSD. The sizes of a DPPSD can be determined using figure 2-4.

NO. OF ANALYSTS, PROGRAMMERS, OR SPECIALISTS	DPPSD SIZE FOR AN ACTIVITY
5 TO 10	SMALL
11 TO 30	MEDIUM
30 OR MORE	LARGE

Figure 2-4.–DP Programming Support Department Size Configuration.

When an ADP installation is classified as a design/development activity, it functions as a special category for program development activites, and may provide centralized applications systems development and maintenance. The program development is for standard systems that are run at multiple activities throughout the Navy or at a single location providing Navy-wide support. The organizational structure and/or responsibilities may vary considerably, but the primary function is responsibility for applications design and development.

For an installation to have a technical support department (TSD) the activity must have an organizational element whose primary function is to provide "generalized technical support." Functions performed are normally in support of hardware, a DPID, a DPPSD, or generalized software which supports multiple applications, as opposed to supporting a specific user application. Functions which may be performed in a TSD include systems software acquisition, installation, testing, distribution and maintenance, performance monitoring, configuration planning, teleprocessing services, and standards and procedures. The sizes of a TSD can be determined using figure 2-5.

EQUIPMENT ORGANIZATION

There are many organizational planning needs to be met when a new installation is to be established or an existing system modified. Planning for the incoming hardware is concerned primarily with space, arrangement, and environment. In most cases planning for hardware installation is fairly routine. The specifications for each unit's required spacing (for repair access) and environment (air circulation, cooling, humidity, raised floor, etc.) are detailed by the manufacturer.

NO. OF ANALYSTS, PROGRAMMERS, OR SPECIALISTS	TSD SIZE FOR AN ACTIVITY
1 TO 5	SMALL
5 TO 15	MEDIUM
15 OR MORE	LARGE

Figure 2-5.–Technical Support Department Size Configuration.

The arrangement of equipment should be of special concern to the senior DP. If possible locate a noisy printer outside the system area. The harsh printer noise and paper lint/dust may be harmful to personnel and may contaminate system hardware. Other problems concerning hardware can usually be resolved by consulting specification books, manufacturers' representatives, and Data System's Technicians.

NONTACTICAL ADP ORGANIZATION

In 1975, a General Accounting Office (GAO) report was very critical of the ADP structure in the Navy. Because of the report, the Navy conducted a reorganization study during 1976. As enumerated by the Vice Chief of Naval Material in 1976, the top 10 ADP problems besetting the Navy were:

1. ADP configuration management–There was no control over the use of computer capacity. Many times the capacity was exhausted by local techniques.
2. Low thresholds–Everything had to be justified; therefore, staffs were swamped with paperwork.
3. Improper support of new projects–New projects were locally received without the addition of necessary resources.
4. Economic justification–This frequently prevented standardization across command lines.
5. Lack of Navy-wide hardware standardization–This command-line problem was created by the differences in development time of large-scale systems.
6. Nonstandardization of systems–This was another command-line problem. Many activities duplicated what other commands or activities had already done.
7. Insufficient overhead to properly manage ADP–Overhead, in this instance,

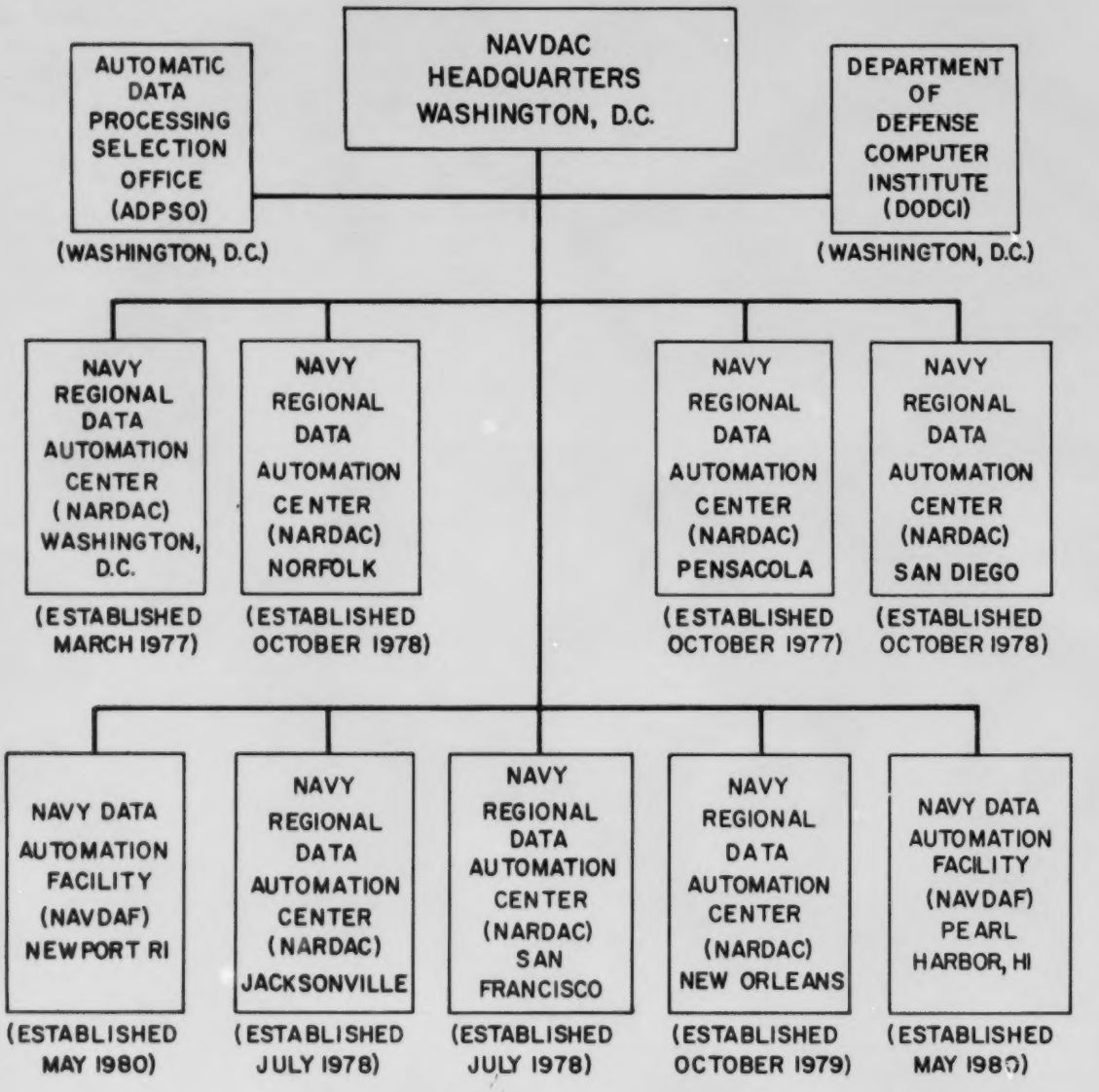
referred to personnel cutbacks that tended to reduce the management and planning staffs.

8. Lack of Navy-wide telecommunications planning.

9. Lack of standard procedures for requesting ADP services and managing systems development.

10. Lack of technical standards and enforcement of them.

The study resulted in the formation of the Naval Data Automation Command as a second-echelon command of the CNO, effective 1 January 1977. Third-echelon commands under NAVDAC are ADPSO (the ADP Selection Office of the Navy), DODCI (the DOD Computer Institute), and a system of from six to eight Regional Data Automation Centers (NARDAC). (See fig. 2-6.)


NAVDAC HEADQUARTERS WASHINGTON, D.C.
AUTOMATIC DATA PROCESSING SELECTION OFFICE (ADPSO)
(WASHINGTON, D.C.)
DEPARTMENT OF DEFENSE COMPUTER INSTITUTE (DODCI)
(WASHINGTON, D.C.)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) WASHINGTON, D.C.
(ESTABLISHED MARCH 1977)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) NORFOLK
(ESTABLISHED OCTOBER 1978)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) PENSACOLA
(ESTABLISHED OCTOBER 1977)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) SAN DIEGO
(ESTABLISHED OCTOBER 1978)
NAVY DATA AUTOMATION FACILITY (NAVDAF) NEWPORT RI
(ESTABLISHED MAY 1980)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) JACKSONVILLE
(ESTABLISHED JULY 1978)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) SAN FRANCISCO
(ESTABLISHED JULY 1978)
NAVY REGIONAL DATA AUTOMATION CENTER (NARDAC) NEW ORLEANS
(ESTABLISHED OCTOBER 1979)
NAVY DATA AUTOMATION FACILITY (NAVDAF) PEARL HARBOR, HI
(ESTABLISHED MAY 1980)

78.167

Figure 2-6.–NAVDAC Commands.

NAVDAC's principal objectives are to improve the effectiveness of ADP systems in support of Navy operations; to exploit all the potentials of ADP and teleprocessing technology in multicommand and multifunctional ADP systems; and to improve the overall management of the Navy's ADP resources.

NAVDAC's mission, as approved by the CNO, entails:

1. Collaboration on ADP matters with all Navy ADP claimants.

2. Approval of systems development, and acquisition and development of ADP equipment and service contracts.

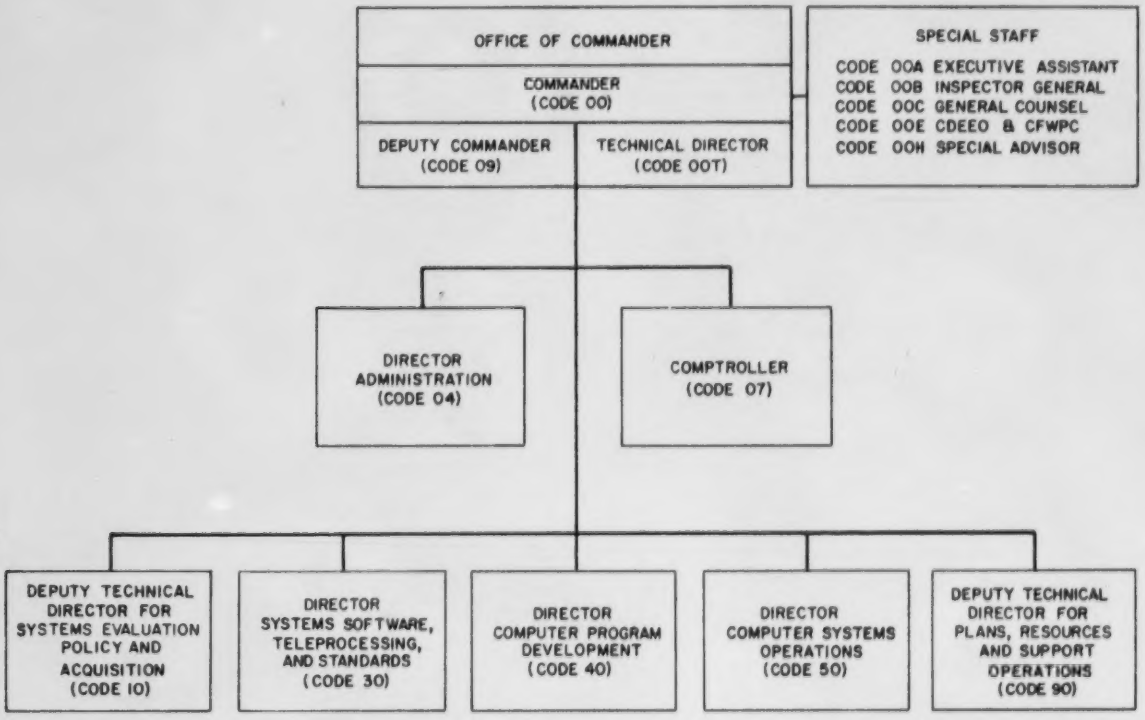
3. Sponsoring ADP technology.

4. Career development and training of personnel.

5. Technical management of all Navy ADP activities.

6. Navy-wide ADP policy, plans, and procedures.

NAVDAC, in brief, is charged with fostering broad-based improvement in the contribution of nontactical ADP to Navy operational effectiveness. NAVDAC's goals include better planning and coordination (Navy-wide) to anticipate, budget for, and satisfy ADP requirements before rather than after they become critical; standardization of systems and consolidation of facilities where it makes good sense; more aggressive and consistent exploitation of computers and teleprocessing; career development of ADP professional personnel; and the formulation of more responsive, up-to-date policy and procedures for the acquisition and management of ADP resources. A summary of organizational structure can be viewed in figure 2-7.


OFFICE OF COMMANDER
COMMANDER (CODE 00)
DEPUTY COMMANDER (CODE 09)
TECHNICAL DIRECTOR (CODE 00T)
SPECIAL STAFF
CODE 00A EXECUTIVE ASSISTANT
CODE 00B INSPECTOR GENERAL
CODE 00C GENERAL COUNSEL
CODE 00E CDEEO & CFWPC
CODE 00H SPECIAL ADVISOR
DIRECTOR ADMINISTRATION (CODE 04)
COMPTROLLER (CODE 07)
DEPUTY TECHNICAL DIRECTOR FOR SYSTEMS EVALUATION POLICY AND ACQUISITION (CODE 10)
DIRECTOR SYSTEMS SOFTWARE, TELEPROCESSING, AND STANDARDS (CODE 30)
DIRECTOR COMPUTER PROGRAM DEVELOPMENT (CODE 40)
DIRECTOR COMPUTER SYSTEMS OPERATIONS (CODE 50)
DEPUTY TECHNICAL DIRECTOR FOR PLANS, RESOURCES AND SUPPORT OPERATIONS (CODE 90)

78.168

Figure 2-7.—Naval Data Automation Command Headquarters.

NONTACTICAL ADP SUPPORT

As part of the overall reorganization of the Navy's nontactical ADP resources and management, each Navy Regional Data Automation Center (NARDAC) was formed from existing facilities and operations in a particular geographical area, of which the former Data Processing Service Centers (DPSCs) formed the nucleus. The NARDACs have a significantly broader mission than the DPSCs, and in all cases the NARDACs were expanded in scope and responsibility, including assignment of Navy-wide areas of ADP technical management responsibilities.

The NARDACs provide a wide range of ADP support services, from assisting potential customers in defining their requirements to providing a modern, on-line, real-time teleprocessing environment in which users do their data processing.

Each NARDAC is organized under a standard structure patterned after NAVDACs. NARDACs are also standardized with ADP capability with the UNIVAC ADPE, specifically the U1100/40. The standardized ADPE gives the NARDACs the means to respond rapidly, efficiently, and economically to the user requirements in the field.

The NARDACs have facilities geographically removed from the NARDAC. These sites, called NAVDAFs (Navy Data Automation Facilities), are located in such areas as Pearl Harbor, Hawaii, and Great Lakes, Illinois. They provide onsite support to major Navy commands/activities in areas not otherwise supported by NARDACs or having special support requirements. The NAVDAFs also have an organizational structure patterned by NARDAC.

CHAPTER 3

ADP PHYSICAL SECURITY, RISK MANAGEMENT, AND PRIVACY

This chapter provides basic information about automatic data processing physical security and risk management, and covers the Privacy Act of 1974. Authoritative references are cited throughout the chapter and are to be utilized when implementing any type of security measures. This chapter should not be used as authority to implement any security measure. It is intended to assist the DPI and DPC in defining specific ADP physical security requirements. Additionally, it lists referenced instruction(s)/manual(s) for developing and implementing sound physical security programs, and establishes and provides background training for conducting audits of these programs.

PHYSICAL SECURITY PROGRAMS

Every ADP organization has, or should have, an on-going physical security program. The majority of these programs differ as the needs, requirements, and locations of the commands differ. The physical security program for a highly classified defense command would not be comparable with the physical security program of an unclassified, nontactical command. Also, a physical security program for an ADP facility in Florida would not require as much emphasis on earthquake protection measures as would an ADP facility in California. Planning a physical security program is as important as actually implementing the program.

The DP technical manager of an ADP facility will derive the most from this chapter if security is designated as an on-going operational function and if an adequate staff is provided to support the function. The general guidelines suggested here for developing and implementing a physical security program can be summarized as follows:

1. Analyze risk as the basis for development of a security policy.
2. Select and implement appropriate security measures to reduce exposure to losses.
3. Develop contingency plans for back-up operations, disaster recovery, and emergencies.
4. Provide indoctrination and training for personnel.
5. Plan and conduct continuing tests and audits and adjust security measures and contingency plans as needed.

ADP THREATS

When planning a physical security program, the DP technical manager should be aware of all the types of threats that may be encountered. Not every Navy ADP facility will be faced with each type of threat, especially if the facility is aboard ship. The impact of a given threat may depend on the geographic location of the ADP facility (earthquakes), the local environment (flooding), and potential value of property or data to a thief, or the perceived importance of the facility to activists and demonstrators or subversives. Not all threats and preventative measures can be discussed in this chapter. For a thorough review of the subject, refer to FIPS PUB 31 and OPNAVINST 5510.45 series. Some of the natural and unnatural threats include:

1. Unauthorized access by persons to specific areas and equipment for such purposes as theft, arson, vandalism, tampering, circumventing of internal controls, or improper physical access to information.

2. ADP hardware failures.

3. Failure of supporting utilities, including electric power, air conditioning, communications circuits, elevators, and mail conveyors.

4. Natural disasters, including floods, windstorms, fires, and earthquakes.

5. Accidents causing the nonavailability of key personnel.

6. Neighboring hazards such as close proximity to chemical or explosive operations, airports, high crime areas, etc.

7. Tampering with input, programs, and data.

8. The compromise of data through interception of acoustical or electromagnetic emanations from ADP hardware.

The preceding list of threats to the operation of an ADP facility contains only a few of the reasons why each command should have an on-going physical security program that is adapted to/tailored to its individual needs and requirements. Only the most likely and common threats are discussed in this chapter.

RISK ANALYSIS

It is recommended that the ADP facility upper management begin development of the physical security program with a risk analysis. A risk analysis, as related to this chapter, is the study of potential hazards that could threaten the performance, integrity, and normal operations of an ADP facility. Experience at various commands has shown that a quantitative risk analysis produces the following benefits:

1. Objectives of the security program are directly related to the missions of the command.

2. Those charged with selecting specific security measures have quantitative guidance on the type and amount of resources that it is reasonable to expend on each security measure.

3. Long-range planners receive guidance in applying security considerations to such things as site selection, building design, hardware configurations and procurements, software systems, and internal controls.

4. Criteria are generated for designing and evaluating contingency plans for backup operations, recovery from disaster, and dealing with emergencies.

5. An explicit security policy can be generated which identifies what is to be protected, which threats are significant and who shall be responsible for execution, review, and reporting of the security program.

Loss Potential Estimates

The first step to be considered when preparing the risk analysis is to estimate the potential losses to which the ADP facility is exposed. The objective of the loss potential estimate is to identify critical aspects of the ADP facility operation and to place a monetary value on the loss estimate. Losses may result from a number of possible situations, such as:

1. Physical destruction or theft of tangible assets. The loss potential is the cost to replace lost assets and the cost of delayed processing.

2. Loss of data or program files. The loss potential is the cost to reconstruct the files either from backup copies if available or from source documents and possibly the cost of delayed processing.

3. Theft of information. The loss potential here is difficult to quantify. Although the command itself would sustain no direct loss, it clearly would have failed in its mission. In some cases, information itself may have market value, for example, a proprietary software package or a name list which can be sold.

4. Indirect theft of assets. If the ADP system is used to control other assets such as cash, items in inventory, or authorization for performance of services, then it may also be used to steal such assets. The loss potential would be the value of such assets which might be stolen before the magnitude of the loss is large enough to assure detection.

5. Delayed processing. Every application has some time constraint, and failure to complete it on time causes a loss. In some cases the loss potential may not be as obvious as, for example, a delay in issuing military paychecks.

The ADP DP technical manager and upper management should construct a table of replacement costs for the physical assets of the ADP facility. This usually includes the building itself and all contents.

Preparation of this tabulation, broken down by specific areas helps to identify areas needing special attention. While the contents of the typical office area may be valued at $5 to $10 per square foot, it is not unusual to find that the contents of a computer room are worth $500 to $2000 per square foot. The estimate is also helpful in planning for recovery in the event of a disaster.

The remaining four loss potential types previously listed are dependent on the characteristics of the individual data processing tasks performed by the ADP facility. The ADP DP technical manager should review each task to establish which losses the facility is exposed to and which factors affect the size of the potential loss. The DP technical managers should call on users to help make these estimates.

In order to make the best use of time, the ADP DP technical manager should do rapid, preliminary screening in order to identify the tasks which appear to have significant loss potential. A table of preliminary estimates is shown in figure 3-1.

Having made a preliminary screening to identify the critical tasks, the ADP DP technical manager should seek to quantify loss potential more precisely with the help of user representatives familiar with the critical tasks and their impact on other activities. Mishaps and losses that could occur should be considered, on the assumption that if something can go wrong, it will. The fact that a given task has never been tampered with, used for an embezzlement, or changed to mislead management in the command is no assurance that it never will be. At this stage of the risk analysis, all levels of management should assume the worst.

Threat Analysis

The second step of the risk analysis is to evaluate the threats to the ADP facility. Threats and the factors which influence their relative importance were outlined earlier in this chapter. Details of the more common threats are discussed later in this chapter and, to the extent it is available, general information about the probability of occurrence is given. These data, the application of common sense, and higher authority instructions/manuals should be used by the DP technical manager to develop estimates of the probability of occurrence for each type of threat.

TASK NAME	RUN TIME	FILE RECON-STRUCTION	CLASSIFIED/ SENSITIVE DATA	PRIOR COMPROMISE/ THEFT OF INFO	DELAYED PROCESSING IMPACT	PROJECT	MANPOWER COST ESTIMATE
R	1.5/D	Easy	No	No	Extreme	Payroll	1 day
S	On line	V. Diff	Yes	Yes	Extreme	Operations	8 hours
T	2.0/D	Difficult	Yes	No	Moderate	Inventory	1 week
U	0.5/W	Normal	No	No	Low	Research	6 days
V	0.7/M	Difficult	Yes	No	Very low	Research	2 days
W	4.5/W	Easy	No	No	Moderate	Inventory	3 hours

Figure 3-1.–Preliminary Estimates of Loss Potential.

While the overall risk analysis should be conducted by the ADP DP technical manager, other personnel at the ADP facility can contribute to the threat analysis and their help should be solicited. Figure 3-2 includes a list of common threats at a shore ADP facility, with space allowed for the agency or individual to contact should the need arise and a corresponding telephone number for each. The DP technical manager should fill in a similar list with local contacts of help and information.

Annual Loss Expectancy

The third step in the risk analysis is to combine the estimates of the value of potential loss and probability of loss to develop an estimate of annual loss expectancy. The purpose is to pinpoint the significant threats as a guide to the selection of security measures and to develop a yardstick for determining the amount of money which is reasonable to spend on each of them. In other words, the cost of a given security measure should relate to the loss(es) against which it provides protection.

To develop the annual loss expectancy, a matrix of threats and potential losses can be constructed. At each intersection, ask if the given threat could cause the given loss. For example, fire, flood, and sabotage do not cause theft-of-information losses, but, in varying degrees, all three result in physical destruction losses and losses due to delayed processing. Likewise, internal tampering could cause an indirect loss of assets. In each case where there can be significant loss, the loss potential is multiplied by the probability of occurrence of the threat to generate an annual estimate of loss.

COMMON THREATS	SOURCES OF LOCAL INFORMATION AND HELP	LOCAL PHONE NUMBER
Fire		
Flood		
Earthquake		
Windstorm		
Power failure		
Air conditioning failure		
Communications failure		
ADP hardware failure		
Intruders, vandals		
Compromising emanations		
Internal theft		
Internal misuse		

Figure 3-2.—Threat help list.

Selecting Remedial Measures

When the estimate of annual loss has been completed, ADP upper management will have a clear picture of the significant threats and critical ADP tasks. The response to significant threats can take one or more of the following forms:

1. Alter the environment to reduce the probability of occurrence. In an extreme case, this could lead to relocation of the ADP facility to a less exposed location. Alternatively, a hazardous occupancy adjacent to or inside the ADP facility could be moved elsewhere.
2. Erect barriers to ward off the threat. These might take the form of changes to strengthen the building against the effects of natural disasters, saboteurs, or vandals. (See OPNAVINST 5510.1 series and 5510.45 series for evaluation guidelines.) Special equipment can be installed to improve the quality and reliability of electric power. Special door locks, military guards, and intrusion detectors can be used to control access to critical areas.
3. Improve procedures to close gaps in controls. These might include better controls over operations or more rigorous standards for programming and software testing.
4. Early detection of harmful situations permits more rapid response to minimize damage. Fire and intrusion detectors are both typical examples.
5. Contingency plans permit satisfactory accomplishment of command missions following a damaging event. Contingency plans include immediate response to emergencies to protect life and property and to limit damage, maintenance of plans and materials needed for backup operation offsite, and maintenance of plans for prompt recovery following major damage to or destruction of the ADP facility. The command's Disaster Control Plan should coincide with the ADP facility's contingency plans.

There are two criteria for selecting specific remedial measures.

1. The annual cost is to be less than the reduction in expected annual loss which could be caused by threats.
2. The mix of remedial measures selected is to be the one having the lowest total cost.

The first criterion simply says that there must be a cost justification for the security program–that it returns more in savings to the ADP facility than it costs. This may seem obvious but it is not uncommon for an ADP manager to call for a security measure, to comply with higher authority security instructions and directives, without first analyzing the risks.

The second criterion reflects the fact that a given remedial measure may often be effective against more than one threat. (See fig. 3-3.)

REMEDIAL MEASURES	THREATS				
	Fire	Internal theft	External theft	Hurri-cane	Sabotage
Fire detection system	X				X
Loss control team	X			X	X
Roving guard patrol	X	X	X		X
Intrusion detectors		X	X		X
Personnel screening		X			X
On-site power generator				X	X
Back-up plan	X			X	X

Figure 3-3.–Remedial Measures.

Since a given remedial measure may affect more than one threat, the lowest cost mix of measures probably will not be immediately obvious. One possible way to make the selection is to begin with the threat having the largest annual loss potential. Consider possible remedial measures and list those for which the annual cost is less than the expected reduction in annual loss. (Precision in estimating cost and loss reduction is not necessary at this point.) If two or more remedial measures would cause a loss reduction in the same area, list them all, but note the redundancy. Repeat the process for the next most serious threat and continue until reaching the point where no cost justifiable measure for a threat can be found. If the cost of a remedial measure is increased when it is extended to cover an additional threat, the incremental cost should be noted. At this point, there exists a matrix of individual threats and remedial measures with estimates of loss reductions and costs, and thus an estimate of the net saving. This can be shown graphically, as in figure 3-4.

For each threat, the estimated loss reduction, the cost of the remedial measure, and the net loss reduction have been given (in that order). By applying remedial measure J to threat A at a cost of $9,000, a loss reduction of $20,000 can be expected (a net saving of $11,000). Furthermore remedial measure J will reduce the threat B loss by $10,000 at no additional cost and the threat C loss by $4,000 at an added cost of only $1,000. Finally, though, it appears that it would cost more than it would save to apply J to threat D. Therefore,

REMEDIAL MEASURES	THREATS											
	A			B			C			D		
J	20*	9	11	10	0	10	4	1	8	2	5	-3
K	20*	15	5	12	0	12	6	0	6	4	2	2

*Same effect.

Figure 3-4.—Threat matrix.

J would not be implemented for D. The net loss reduction from J could be expressed as:

$$J(A,B\&C) = 11 + 10 + 3$$

$$= \$24,000$$

The table indicates that J and K have the same reduction effect on threat A. Since K costs more than J, it might, at first glance, be rejected. However,

$$K(A,B,C\&D) = 5 + 12 + 6 + 2$$

$$= \$25,000$$

and

$$J(A,B\&C) + K(A,B,C\&D) = -4 + 22 + 9 + 2$$

$$= \$29,000$$

Therefore, while J and K are equally effective on threat A, K appears to be more effective than J on the other threats. Further checking shows that their combined use results in the greatest overall net loss reduction.

By going through the process just described, using preliminary estimates for cost and loss reduction, a DP technical manager can test various combinations of remedial measures, and thus identify the subset of remedial measures which appears to be the most effective. At this point, the DP technical manager should review the estimates and refine them as necessary to ensure compliance with higher authority security instructions.

If all of the preceding procedures have been followed, the following factors will have been established and documented:

1. Significant threats and probabilities of occurrence

2. Critical tasks and the loss of potential related to each threat on an annual basis

3. A list of remedial measures which will yield the greatest net reduction in losses, together with their annual cost

With this information at hand, ADP upper management can move ahead with implementation of the physical security program. Since the analysis of remedial measures will have identified those with the greatest impact, relative priorities for implementation can also be established.

IMPLEMENTING A SECURITY PROGRAM

The use of a risk analysis and higher authority instructions has been suggested as the basis for developing an ADP security program. Even though implementation of the program depends on local instructions/directives and conditions, it may not be clear just where to begin. Following is a suggested outline that can be used as a basis for planning an ADP security program.

1. Preliminary planning. Establish an ADP security team to prepare an ADP security program and make responsibility assignments.
2. Perform a preliminary risk analysis to identify major problem areas.
3. Select and implement urgent "quick fix" security measures as needed.
4. Perform and document a detailed risk analysis for review and approval.
5. Based on the approved risk analysis selected, justify cost and document action plans with budgets and schedules for security measures, contingency plans, training and indoctrination plans, and test and audit plans.
6. Carry out the approved action plans.
7. Depending on the results of tests, audits, and changes in mission or environment, repeat the detailed risk analysis and subsequent steps on a regular (at least annual) basis.

The action plans should include adequate documentation. For example, the documentation might include:

1. A security policy statement which provides general guidance and assigns responsibilities.
2. A security handbook with instructions that describe in detail the security program and procedures and the obligations of ADP personnel, users, and supporting personnel.
3. Command standards for system design, programming, testing, and maintenance to reflect security objectives and requirements.
4. Contingency plans for backup operations, disaster recovery, and emergency response.
5. Booklets or command instructions for ADP staff indoctrination in security program requirements.

Depending on the normal practice of the ADP facility, these documents may be completely separate items or may be included in other documents. For example, emergency response plans for the ADP facility might be included in the command's Disaster Control Plan. Similarly, security standards could be added to existing documents.

The final point to be made is the importance of continuing an audit and review of the security program. A major effort is required for the initial risk analysis, but once it has been completed, a regular review and updating can be done much more quickly. By evaluating changes in command mission, the local environment, the hardware configuration, and tasks performed, the DP technical manager can determine what changes, if any, should be made in the security program to keep it effective.

Authoritative Reference

There are numerous higher authority instructions for physical security, data protection, and security in general that the DP technical manager should have a thorough knowledge of before implementing any security plan. The DP technical manager should reference the following instructions and manuals when making security decisions and also when studying for advancement in rate:

1. OPNAVINST 5239.1 series with enclosures, Department of the Navy security program for automatic data processing systems
2. FIPS PUB 65 (encl. (3) to OPNAVINST 5239.1 series) Guideline for automatic data processing risk analysis

3. OPNAVINST 5510.1 series, Department of the Navy Information Security Program Regulations

4. Office of Naval Intelligence (ONI-CS-63-1-76), Guide for Security Equipment

NATURAL DISASTERS

Fires, floods, windstorms, and earthquakes all tend to have the same basic effects on ADP operations. These effects are the physical destruction of the facility and its contents and interruption of normal operations. They also represent a threat to the life and safety of the ADP staff. Fire is the only natural disaster that will be discussed in this chapter.

FIRE SAFETY

Experience over the last two decades has demonstrated the sensitivity of ADP facilities to fire damage resulting in disruption of operations. A number of major losses have involved noncombustible buildings. In those cases where vital tapes were safeguarded and the computer hardware was relatively uncomplicated, rapid recovery was possible, often in a matter of days. However, it seems likely that if a large computer configuration, such as a World Wide Military Command and Control System (WWMCCS), were destroyed or if backup records were inadequate, recovery would be a lengthy process that could take many weeks or months.

Fire safety should be a key part of the ADP facility's physical security program and should include these elements:

1. Location, design, construction, and maintenance of the ADP facility to minimize the exposure to fire damage.
2. Measures to ensure prompt detection of and response to a fire emergency.
3. Provision for quick human intervention and adequate means to extinguish fires.
4. Provision of adquate means and personnel to limit damage and effect prompt recovery.

Facility Fire Exposure

The first factor to consider in evaluating the fire safety of an ADP facility is what fire exposure results from the nature of the occupancy (material) of adjacent buildings and the ADP facility building. Generally speaking, the degree of hazard associated with a given occupancy (material) depends on the amount of combustible materials, the ease with which they can be ignited, and the likelihood of a source of ignition.

The second and third fire safety factors are the design and construction of the building. There are five basic types of construction described in figure 3-5, with the approximate destruction time shown for each fire classification.

The actual performance of a building will depend not only on the type of construction, but on design details such as:

1. Fire walls which in effect divide a structure into separate buildings with respect to fires.
2. Fire rated partitions which retard the spread of a fire within a building.
3. Fire rated stairwells, dampers, or shutters in ducts; fire stops at the junction of floors, and walls and similar measures to retard the spread of smoke and fire within a building.
4. Use of low-flame spread materials for floor, wall, and ceiling finish to retard propagation of flame.

Type of Construction	Approximate Fire Classification
Fire Resistant	2 or 3 hours
Heavy Timber	1 plus hours
Noncombustible	1 hour
*Ordinary Construction	Less than 1 hour
Wood Frame	Minutes

*depends on size of timber used.

Figure 3-5.—Types of construction.

It should be understood that this discussion has been much simplified. However, consideration of these factors as they apply to an existing or projected ADP facility will help to determine the amount of attention that should be payed to fire safety. Seek the assistance of a qualified fire protection engineer or local base fire personnel in evaluating the inherent fire safety of the ADP facility and identifying hazards.

The July 1973 fire at the U.S. Military Personnel Records Center, Overland, Missouri, was an unfortunate demonstration of the result when well-tested fire safety design criteria are disregarded in overemphasizing protection against other risks. Lack of sprinkler protection, inadequate access to the fire site, and related design deficiencies seriously hampered fire fighting and in the end resulted in much more damage to records than would have resulted from the operation of sprinkler heads.

The fourth factor in fire safety is the way in which the building is operated. It should be understood that the inherent fire safety of a building can be rendered ineffective by careless operation. This includes: fire doors propped open; undue accumulation of debris or trash; careless use of flammable fluids, welding equipment, and cutting torches; substandard electric wiring; inadequate maintenance of safety controls on ovens and boilers; and excessive concentration of flammable materials. ADP facilities for example, have a particular hazard from the accumulation of lint from card and paper operations. The ADP physical security program should strive, in coordination with the building maintenance staff, to identify and eliminate such dangerous conditions. Futhermore, it should be understood that this must be a continuing effort and a consideration in the assignment of security management responsibilities. The security audit plan should include verification of compliance with established standards.

Fire Detection

Despite careful attention to the location, design, construction, and operation of the ADP facility, there is still the possibility that a fire can start. Experience has shown repeatedly that prompt detection is a major factor in limiting fire damage. Typically, a fire goes through three stages. Some event, such as a failure of electrical insulation, causes ignition. An electrical fire will often smolder for a long period of time. When an open flame develops, the fire spreads through direct flame contact, progressing relatively slowly, with a rise in the temperature of the surrounding air. The duration of this stage is dependent on the combustibility of the materials at and near the point of ignition. Finally, the temperature reaches the point at which adjacent combustible materials give off flammable gases. At this point the fire spreads rapidly and ignition of nearby materials will result from heat radiation as well as direct flame contact. Because of the high temperatures and volumes of smoke and toxic gases associated with this third stage, fire fighting becomes increasingly difficult and often people cannot remain at the fire site.

Given the objective to discover and deal with a fire before it reaches the third stage, one can see the limitation of fire detection which depends on detecting a rise in air temperature. It is for this reason that the areas in which electronic equipment is installed be equipped with products-of-combustion (smoke) detectors. Such detectors use electronic circuitry to detect the presence of abnormal constituents in the air which are usually associated with combustion.

To be effective in providing prompt detection, the following points should be considered in designing a fire detection system:

1. The location and spacing of detectors should take into consideration the direction and velocity of air flow, the presence of areas with stagnant air, and the location of equipment and other potential fire sites. Note that detectors may be required under the raised floor, above the hung ceiling, and in air conditioning ducts as well as at the ceiling. It may also be wise to put detectors in electric and telephone equipment closets and cable tunnels.

2. The design of the detection control panel should make it easy to identify the detector which has alarmed. This implies that the detectors in definable areas (for example,

the tape vault, the east end of the computer room, and administrative offices) should be displayed as a group on the control panel. In other words, when an alarm sounds, inspection of the control panel should indicate which area or zone caused the alarm. Generally, and preferably, each detector will include a pilot light which lights when the detector is in the alarm state. In some cases there should be a separate indicator light at the control panel for each detector. It is also important to see that the alarm system itself is secure. Its design should cause a trouble alarm to sound if any portion of it fails, or if there is a power failure. Steps should be taken to assure that the system can not be deactivated readily, either maliciously or accidentally.

3. Meaningful human response to the detection and alarm systems is necessary if they are to be of any value. This means that the fire detection system should be designed to assure that someone will always be alerted to the fire. Typically, it is expected that the computer room staff respond to an alarm from the ADP facility alarm system. A remote alarm should also be located at another point in the building, manned at all times, such as the lobby guard post, security center, or building engineer's station. This provides a backup response when the computer area is not occupied. If there is any possibility that the remote alarm point will not be manned at all times, a third alarm point should be located offsite, usually at the nearest fire station or the command's fire department for the facility.

4. Proper maintenance is essential to the fire detection system. The nature of smoke detectors is such that nuisance alarms may be caused by dust in the air or other factors. Thus, there is a tendency to reduce sensitivity in order to eliminate nuisance alarms, with the result that detection of an actual fire may be delayed. To ensure proper operation, it is important to see that qualified personnel (a vendor representative, building engineer, or Public Works Center personnel) verify correct operation at the time of installation, and at least once each year thereafter. Furthermore, each fault condition should be corrected immediately. Unfortunately, there is a common tendency to turn off the fire detection system or silence the alarm bell, creating the danger that there will be no response if a fire should occur.

In addition to alerting personnel to the presence of a fire, the detection equipment can be used to control the air conditioning system. There is some support for the view that, upon detection, air handling equipment should be shut down automatically to avoid "fanning the flames" and spreading smoke. This may not be the best plan, as nuisance alarms will result in needless disruption. A preferred technique may be to cause the system to exhaust smoke by stopping recirculation, and switching to 100-percent outisde air intake and room air discharge. As a rule this can be done by adjustment of air conditioning damper controls and their interconnection with the fire detection system. However, it may be necessary to modify the air conditioning system.

The use of this technique is at the discretion of command policy.

Fire Extinguishment

Fire extinguishment may be accomplished using one or more of the following four methods:

1. Portable or hand extinguishers operated by military or civil service personnel in an effort to control the fire before it gets out of hand.

2. Hose lines used by military, civil service, or professional fire fighters to attack the fire with water.

3. Automatic sprinkler systems which release water from sprinkler heads activated in the temperature range of 135° to 280°F.

4. Volume extinguishment systems which fill the room with a gas that interferes with the combustion process.

To ensure the effectiveness of portable extinguishers, several measures should be observed. Extinguishers should be placed in readily accessible locations, not in corners or behind equipment. Each location should be marked for rapid identification; for example, a large red spot or band can be painted on the wall

or around the column above the point where each extinguisher is mounted. It is important that each DP technical manager ensure proper inspection in accordance with command policy. Each extinguisher should have an inspection tag affixed to it, on which is the signature of the inspecting petty officer or fire marshal and the inspection date.

In all probability, the ADP facility technical manager will want to establish a first line of defense against fire involvement between the time of notification of and response by professional or highly trained fire fighters, and will incorporate this as part of the command's disaster control plan. Every command, regardless of size, needs military personnel who are knowledgeable and trained in fire safety. Any practical and effective organization for fire protection must be designed to assure prompt action immediately at the point where a fire breaks out. This usually necessitates every organizational unit or area of a command having a nucleus of key personnel who are prepared, through instruction and training, to extinguish fires promptly in their incipient stage. Such individuals become knowledgeable in specialized fire protection and the systems applicable to the facility in question: how to turn in an alarm, which type of extinguisher to use for which type of fire and how to use it. Further, such individuals can serve as on-the-job fire inspectors, constantly seeking out, reporting, and correcting conditions that may cause fires. They can help ensure that fire fighting equipment is properly located and maintained, that storage does not cause congestion which could hamper fire fighting, and that general housekeeping is maintained at a reasonably high level to minimize fire risk.

SUPPORTING UTILITIES

Every Navy ADP facility is dependent upon supporting utilities such as electric power and air-conditioning and may have to depend on communication circuits, water supplies and elevators for its operation. Not all commands are self-sufficient; they contract some or all of these utilities from civil sources. In using these utilities, the DP technical manager should consider the probability of occurrence and the effects of breakdowns, sabotage, vandalism, fire, and flooding. These effects can then be related to the needs of the ADP facility as established by the risk analysis.

ELECTRIC POWER

Variations of a normal waveform in the electric power supply can affect the operation of ADP hardware. The ADP hardware rectifies the alternating current, filters, and voltage regulates the resulting direct current, and applies it to the ADP circuitry. The filtering and regulation cannot be expected to eliminate voltage variations beyond a reasonable range. If line voltage is 90 percent or less of nominal for more than 4 milliseconds, or 120 percent or more of nominal for more than 16 milliseconds, excessive fluctuations can be expected in the d.c. voltage applied to the hardware circuitry. This power fluctuation causes unpredictable results on hardware, logic, and data transfer. These power line fluctuations, referred to as transients, are usually caused by inclement weather.

Internally generated transients depend on the configuration of power distribution inside the ADP facility. The effects of internal transients can be minimized by isolating the ADP hardware from other facility loads. Ideally, the computer area power distribution panels should be connected directly to the primary feeders and should not share step-down transformers with other high-load equipment.

The risk analysis should include a complete power transient and failure study. It should also take into careful consideration the projected growth in particularly sensitive applications (such as real time or teleprocessing) in projecting future loss potential.

In some cases it may be economically feasible to connect the ADP facility to more than one utility feeder via a transfer switch. Thus if one feeder fails, the facility's load may be transferred to the alternate feeder. This technique is of greater value if the two feeders connect to different power substations.

If the ADP facility is in a remote area, an uninterrupted power supply (UPS) usually is required as a backup power source. The UPS system can be manually or automatically controlled from prime power sources or from the ADP computer site. The typical UPS consists of a solid-state rectifier which keeps batteries charged and drives a solid-state invertor. The inverter synthesizes alternating current for the computer. A simplified block diagram is shown in figure 3-6.

Depending on the ampere-hour capacity of the battery (or batteries), the UPS can support its load for a maximum of 45 minutes without prime power source input electricity. At the same time, it will filter out transients. To provide extra capacity to protect against a failure of the UPS, a static transfer switch can be inserted between the UPS and the computer, as shown in figure 3-7. The control circuitry for the static switch can sense an overcurrent condition and switch the load to the prime power source without causing a noticeable transient.

If the facility's current needs exceed its capacity, it may be economically feasible to use multiple, independent UPS units, as shown in figure 3-8. Since each unit has its own disconnect switch, it can be switched offline if it fails.

Finally, if the risk analysis has shown a major loss from power outages lasting 30 to 45 minutes or beyond, an onsite generator can be installed as shown in figure 3-9. The prime mover may be a diesel motor or a turbine. When the external power fails, UPS takes over and the control unit starts the prime mover automatically. The prime mover brings the generator up to speed. At this point, the UPS switches over to the generator. Barring hardware failures, the system supports the connected load as long as there is fuel for the prime mover. Note that the generator must be large enough to support other essential loads, such as air-conditioning or minimum lighting, as well as the UPS load.

When this configuration is used, the DP technical manager should have a close communication liaison with the power plant source to ensure that the generator is coming up to normal speed for the switchover from UPS.

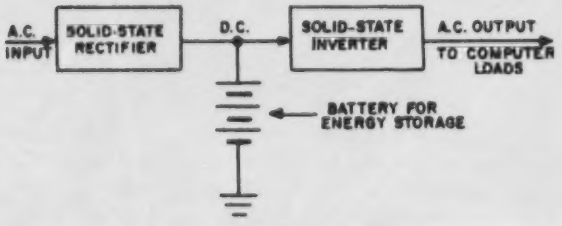


Figure 3-6.—Simplified block diagram of an uninterrupted power supply. (UPS)

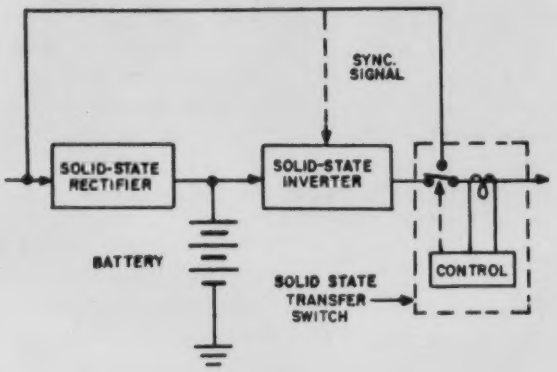


Figure 3-7.—UPS with transfer switch.

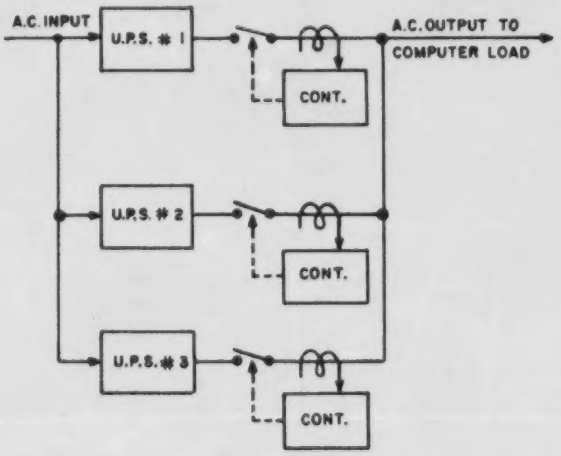
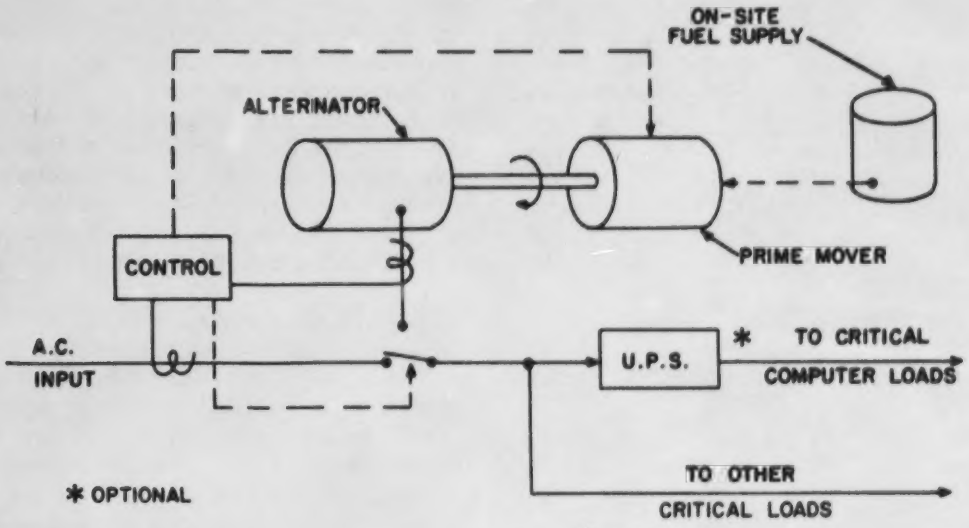


Figure 3-8.—Multiple, independent UPS units.



78.167

Figure 3-9.–UPS with onsite generation.

The UPS system takes over automatically and the change in power source may not be noticed in the ADP facility. However, when the UPS system changes over to the generator it may require a manual power panel setting in the ADP facility by the DP technical manager.

PHYSICAL ADP PROTECTION

The physical protection of the ADP facility can be thought of as the process of permitting access to the facility by authorized persons, while denying access to others. The physical protection of an ADP facility is not as stringent for an ADP facility that processes "unclassified" data as it is for an ADP facility that processes "classified" data. In the following example/discussion, assume that the facility processes classified material and physical protection is afforded in accordance with OPNAVINST 5510.1 series and OPNAVINST 5510.45 series. Particular attention should be paid to applying physical protection and security policy wherever automatic data processing equipment is employed for processing classified information in accordance with OPNAVINST 5239.1 series.

The DP technical manager should ensure that plans are developed for the protection, removal, or destruction of classified material in the case of a natural disaster, civil disturbance, or enemy action. The plans should establish detailed procedures and responsibilities for the protection of classified material so that it does not fall into unauthorized hands in the event of an emergency. They should also indicate what material is to be guarded, removed, or destroyed. An adequate emergency plan for classified material should provide for guarding the material, removing the classified material from the area, complete destruction of the classified material on a phased priority basis, or appropriate combinations of these actions.

The emergency plans should also provide for the protection of classified information in a manner that minimizes the risk of loss of life or injury to ADP personnel. The immediate placement of a trained and preinstructed perimeter guard force around the affected area to prevent the removal of classified material is an acceptable means of protecting the classified material. This action reduces the risk of casualties.

Physical security requirements for the central computer ADP facility area should be commensurate with the highest classified and most restrictive category of information being handled in the ADP system. If two or more computer systems are located in the same controlled area, the equipment comprising each system may be located so that direct personnel access, if appropriate, is limited to a specific system.

BOUNDARY PROTECTION

The threat analysis may indicate the need to protect the property boundary of the ADP facility. This may be accomplished by installing fences or other physical barriers, outside lighting, or perimeter intrusion detectors, or by using a patrol force. Often a combination of two or more of these will be efficient. Fences should be 8 feet high with three strands of barbed wire. Fences provide crowd control, deter casual trespassers, and help in controlling access to the entrances, but they do not stop the determined intruder.

In situations where manpower shortages exist, the fence can be equipped with penetration sensors that should sound an internal alarm only. This type of physical protection system uses small sensors mounted at intervals on the fence and at each gate.

EMANATIONS

In evaluating the need for perimeter protection, the DP technical manager should take into account the possibility that electromagnetic or acoustic emanations from ADP hardware may be intercepted. Tests have shown that interception and interpretation of such emanations may be possible under the right conditions by technically qualified persons using generally available hardware. As a rule of thumb, interception of electromagnetic emanations beyond 300 meters is very difficult. However, if the DP technical manager has reason to believe that there may be a potential exposure to interception, technical guidance should be sought from upper management and the Chief of Naval Operations (OP-009D).

Measures to control compromising emanations are subject to approval under the provisions of DOD Directive S-5200.19 series, by the cognizant authority of the component approving security features of the ADP system. Application of these measures within industrial ADP systems is only at the direction of the contracting activity concerned under provisions of DOD Directive 5200.28 series, and the requirements are to be included in the contract.

INTERIOR PHYSICAL PROTECTION

The Joint-Services Interior Intrusion Detection System (J-SIIDS) is designed to provide reliable detection, on a 24-hour basis, of intrusions, attempted instrusions, and equipment tampering attempts. All components of the J-SIIDS, except for the monitoring and display equipment, contain internal tamper switches that are activated when the component enclosure cover is removed or opened.

The Joint-Services Interior Intrusion Detection System (Fig. 3-10) consists of a family of intrusion and duress sensors, a control unit, monitoring and display equipment consisting of alarm and status monitor modules and monitor cabinets, a secure data transmission system, and an audible alarm. When properly installed, the system detects attempted and actual intrusions and notifies the designated authorities.

The sensors and the control unit are located in a protected area. The control unit receives and processes the alarms from the sensors and supplies power to the sensors. The alarm and status signals after processing, are relayed directly to the audible alarm, if used (except for a duress alarm), and to the monitor modules via the data transmisssion system or directly by unsupervised hardwire connections. The audible alarm normally is mounted on the outside of the room or building being protected and gives notice to personnel in the area that an alarm signal has been generated by the sensors. The monitoring and display equipment normally is located in an area where monitoring personnel are on duty 24 hours a day. The monitoring and display equipment consists of monitor cabinets

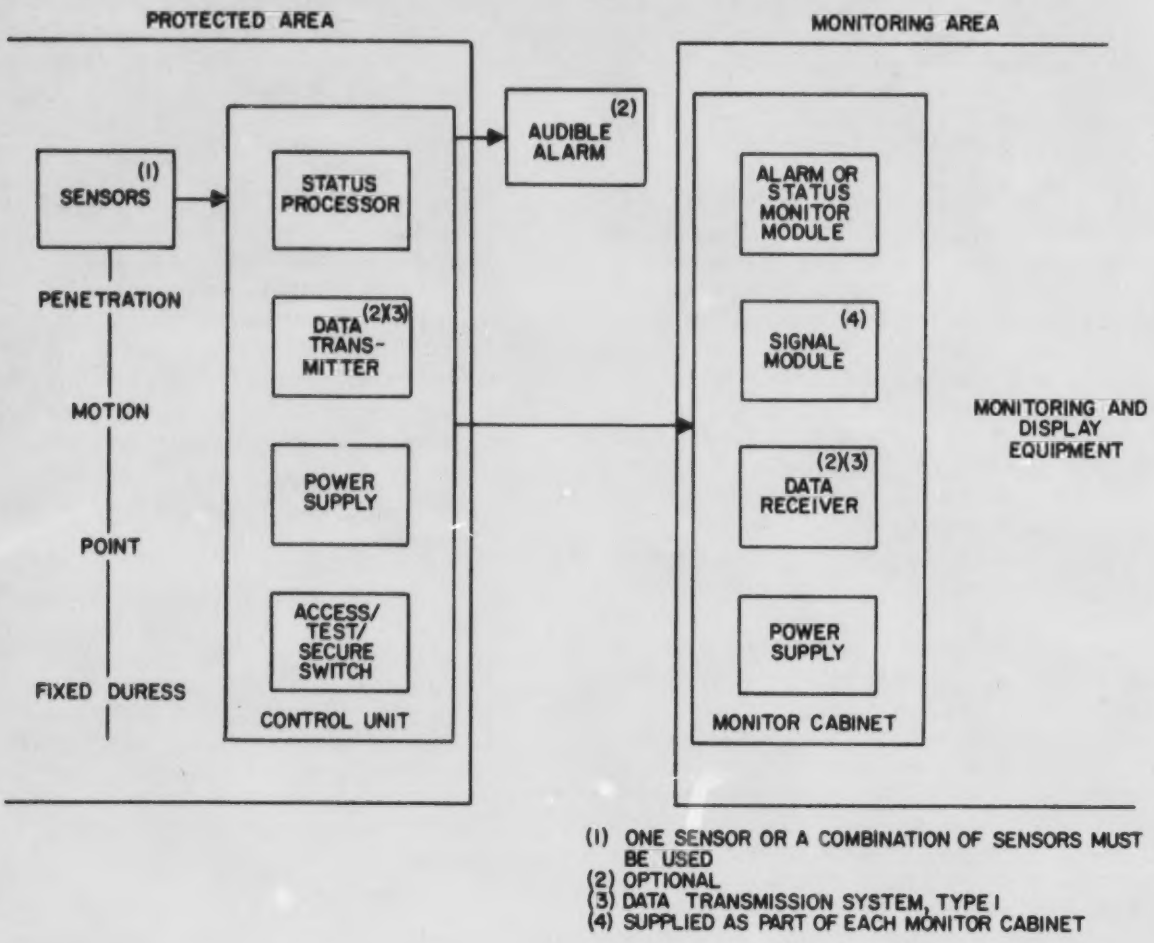


Figure 3-10.–Joint-Services Interior Intrusion Detection System (J-SIIDS).

and status or alarm monitor modules (one for each control unit). The status monitor module gives an audible and visual indication of alarm and status changes. The alarm monitor module gives audible and visual indication only of alarm conditions.

J-SIIDS Components

By using the J-SIIDS components for internal physical security, commands should be better able to select those types of alarm system configurations that best suit their specific requirements. All J-SIIDS components and the use of each are described in the Office of Naval Intelligence publication for the "Guide for Security Equipment," ONI-CS-63-1-76.

REMOTE TERMINAL AREAS

While the physical and personnel security requirements for the central computer facility area are based upon the overall requirements of the total ADP system, remote terminal area requirements are based upon the highest classified and most restrictive category and type

of material which will be accessed through the terminal under system constraints.

Each remote terminal should be individually identified to ensure required security control and protection, with each terminal identified as a feature of hardware in combination with the operating system.

When a peripheral device or remote terminal, whether or not approved for the handling of classified material, is to be used by personnel of a component that is not responsible for the overall operation and control of the ADP system, the security measures for the device or terminal and its area is prescribed by the authority responsible for the security of the overall ADP system. Such security measures are agreed to and implemented before the user's peripheral device or remote terminal is connected to the ADP system.

When one or more DOD's component's ADP systems become a part of a larger ADP network, the approval and the authority to authorize temporary exceptions to security measures for the component's ADP system in the network requires the concurrence and approval of both the DOD component operating the ADP system and the DOD component having overall responsibility for the security of the network.

Each remote terminal which is not controlled and protected as required for material accessible through it, should be disconnected from the ADP system when the system contains classified information.

Disconnect procedures, when required to protect classified material contained in the ADP system, are used to disconnect remote input/output terminals and peripheral devices from the system by a hardware or software method authorized by the designated approving authority of the central computer facility.

PHYSICAL SECURITY SURVEY

An annual physical security survey of the ADP facility's area should be conducted by the DP technical manager. The first step of the survey is to evaluate all potential threats to the ADP facility as discussed earlier in this chapter. The second step of the survey is to define and tabulate areas within the facility for control purposes. Details depend on the specifics of each facility, but the following are common areas which should be considered:

1. Public entrance or lobby
2. Loading dock
3. Spaces occupied by other building tenants
4. ADP facility reception area
5. ADP input/output counter area
6. ADP data conversion area
7. Tape library
8. Systems analysis and programming areas
9. Computer room spaces
10. Communications equipment spaces
11. Air conditioning, UPS, and other mechanical or electrical equipment spaces

The survey should verify security measures already in place and recommend any improvements to upper management. The DP technical manager should obtain a current floor plan which depicts all areas within the facility, and includes all access points and any adjacent areas belonging to the ADP facility, such as parking lots and storage areas. Begin the survey at the perimeter of the ADP facility, considering the following:

1. Property line to include fencing, if any, and type. Note the condition, the number of openings according to type and use, and how they are secured. Are there any manned posts at the property line?

2. Outside parking facilities. Is this area enclosed and are there any controls? Is the parking lot controlled by manned posts or are devices used?

3. Perimeter of facility. Note all vehicular and pedestrian entrances and what controls are used, if any. Check all doors–their number, how they are secured, and any controls or devices, such as alarms or key card devices. Check for all ground floor or basement windows and how they are secured, screening of bars for example, and their vulnerability. Check for other entrances such as vents and manholes. Are they

secured and how? Check for fire escapes–their number and location and accessibility to the interior or the facility from the fire escape (windows, doors, roof). How are accessways secured?

4. Internal security. Begin at the top floor or in the basement. Check for fire alarm systems and devices noting the type, location, and number. Where does the alarm annunciate? Check telephone and electrical closets to see if they are locked. Are mechanical and electrical rooms locked or secured? Note any existing alarms as to type and number. Where do the alarms annunciate? Determine the number and location of manned posts, hours, and shifts.

5. Monitoring facility. Know the location, who monitors, who responds, its type, and the number of alarms being monitored.

The following questions should also be included in a physical security survey:

1. Is the installation/building protected by (an) alarm system(s)?
2. How many zones of protection are within the protected building?
3. Is the alarm system adequate and does it provide the level of protection required?
4. Are there any vulnerable areas, perimeter, or openings not covered by an alarm system?
5. Is there a particular system that has a high nuisance alarm rate?
6. Is the alarm system inspected and tested occasionally to ensure operation?
7. Is the system backed up by properly trained, alert protection personnel who know what steps to take in case of an alarm?
8. Is the alarm system regularly inspected for physical and mechanical deterioration?
9. Does the system have tamper-proof switches to protect its integrity?
10. Is there an environmental or protective housing or cover on the system(s)?
11. Is there an alternate or separate source of power available for use on the system in the event of an external power failure?
12. Where is the annunciating unit located–local, central station, or remote?
13. Who maintains the equipment and how is it maintained (contract, lease equipment, force account personnel, military or civil service)?
14. Is the present equipment outdated?
15. Are records kept of all alarm signals received, including the time, date, location, action taken, and cause of the alarm?
16. Are alarms generated occasionally to determine the sensitivity and the capabilities of systems?

When the physical security survey is completed, it should provide a picture of the existing alarm systems and the location of each, and also the number and location of manned posts, the number of personnel at these posts, and the schedule of each.

With these facts in hand, the DP technical manager can proceed to the evaluation of existing access controls and protection measures, identification of areas where remedial measures are needed, and selection of specific measures.

The use of various types of security hardware devices to augment the existing personnel protective force should always be considered. Through the use of such devices, it may be possible to save on operating cost.

CONTINGENCY PLANNING

Each command of the Navy has an assigned mission. Operation plans and the command's organizational manual are prepared and executed for the accomplishment of that mission. These operation plans assume normal working conditions, the availability of the command's resources and personnel, and a normal working atmosphere. Even so, the DP technical manager should recognize that, despite careful use of preventive measures, there is always some likelihood that events will occur which could prevent normal operations and interfere with the command's mission. For this reason, contingency plans should be included in the ADP security program. For the purpose of this chapter, these contingency plans are referred to as the Continuity of Operations (COOP) Program.

There should be three different types of contingency plans that make up a COOP security program for an ADP facility:

1. Emergency response. There should be procedures for response to emergencies such as fire, flood, civil commotion, natural disasters, bomb threats, enemy attack, etc., in order to protect lives, limit the damage to naval property, and minimize the impact on ADP operations.

2. Backup operations. Backup operation plans are prepared in order to ensure that essential tasks (as identified by the risk analysis) can be completed subsequent to disruption of the ADP and that operations continue until the facility is sufficiently restored or completely relocated.

3. Recovery. Recovery plans should be made to permit smooth, rapid restoration of the ADP facility following physical destruction or major damage.

COOP PREPARATION

It is recommended that each ADP facility establish and appoint members to a formal board to construct, review, and recommend command procedures for approval in creating a COOP program. Figure 3-11 shows suggested tasks and how they may be set up and assigned. Each ADP facility will need to adapt to its own special circumstances and make full use of the resources available to it.

Emergency Response Planning

The term emergency response planning is used here to refer to steps taken immediately after an emergency occurs to protect life and property and to minimize the impact of the emergency. The risk analysis should be reviewed by the DP technical manager to identify emergency conditions which have particular implications for ADP operations, such as protection of equipment during a period of civil commotion and subsequent to a natural disaster (fire or flood, for example). Where civil commotion and natural disaster are found, local instructions should be developed and implemented to meet the special needs of the ADP facility. It is suggested that these instructions and procedures be designated the "Loss Control Plan" and implemented as part of COOP.

Loss control can be particularly important to the ADP facility. In a number of recent fires and floods, the value of being prepared to limit damage has been amply demonstrated. By reviewing operations and the location of critical equipment and records with shift leaders, the DP technical manager can develop measures which can be used in case of an emergency. The guidelines should be similar to the following:

1. Notify online users of the service interruption.
2. Terminate jobs in progress.
3. Rewind and demount magnetic tapes; remove disk packs; clear card readers.
4. Power down ADP hardware and cover with plastic sheeting or other waterproof material.
5. Put tapes, disks, card decks, run books, and source documents in a safe place.
6. Power down air-conditioning equipment.

If evacuation of work areas is ordered or likely, all personnel should be instructed to:

1. Put working papers and other unclassified material in desks or file cabinets and close them.

2. Turn off equipment but leave room lights on.

3. Close doors as areas are evacuated, but ensure that locks and bolts are not secured.

The loss control plan should define the steps to be taken, assign responsibilities for general and specific steps, and provide any needed materials and equipment in handy locations. In some cases, there will be ample time to take all measures, but in extreme emergencies life safety will dictate immediate evacuation. For this reason the loss control plan should designate one or more individuals in each ADP area who, in the event of an emergency, shall determine what can be done to protect equipment and records

	COOP BOARD MEMBERS						
	DP Technical Manager	User Representatives	CO XO GS Upper Management	Security Officer	Supply Division	Public Works Center	Operations Officer (ADP)
1. Establish board members	*		*				*
2. Estimate recovery time	*				*	*	*
3. Failure mode analysis							
ADP hardware	*						*
Utility failure	*			*			*
Fire, flood, wind	*			*			*
4. Loss potential	*	*	*				*
5. Emergency response plans	*		*	*			*
6. Selection of backup modes	*	*	*				*
7. Recovery plans	*	*	*		*	*	*

Figure 3-11.–Organization and tasks for COOP.

without endangering life, and direct ADP staff members accordingly.

Earlier in this chapter, measures were discussed to protect the facility against the effects of fire, flooding, windstorm, and similar natural disasters. The DP technical manager should review, semiannually, protective plans with the operations division officer to assure that all normal requirements and any special requirements of the ADP facility are satisfied. At the same time, the DP technical manager should brief upper management on the ADP facility's plans and status, to get their advice and to ensure good coordination.

When emergency response planning has been completed and approved, it should be documented succinctly for easy execution, as in the following example for a fire emergency.

Fire Emergency Response

1. Report fire (list phone number)
2. Assess life-safety hazard
3. Evacuate facility if necessary
4. Initiate loss control procedures

COOP Backup Planning

The risk analysis should have identified those situations in which backup operations will probably be needed to avoid costly delays in accomplishing the command's mission. The next step is to develop plans for backup operations which are economically, technically, and operationally sound. Details will depend on circumstances at the ADP facility, but some general guidance and suggestions can be helpful in considering the alternatives.

Backup operations may take place onsite when there is only a partial loss of capability, but may require one or more offsite locations when there has been major damage or destruction. The backup procedures may replicate normal operation or be quite different. Quite often ADP mangement, when considering backup, will find that an exact replica of the onsite ADP system is not available for backup or that the time available per day is less than what is needed to complete all assigned tasks. From this it might be concluded that backup is impossible. On the contrary, there are a number of things that can be done to make backup resources available:

1. Fostpone the less urgent tasks. The DP technical manager should tabulate the ADP tasks in descending order or urgency as identified by the risk analysis. Having estimated the time to return to normal following a disruptive event, ADP management can quickly see which tasks can be set aside. These include such things as program development, long cycle (monthly, quarterly or annual) processing, and long-range planning. As long as adequate catch-up time is available after the return to normal, there should be a number of tasks which can be safely postponed.

2. Substitute other procedures. If increased cost or degraded service can be accepted temporarily it may be possible to use other procedures. (For example, a punched card input could be used for a failed OCR unit.) If printer capability is lost, print tapes could be carried to a backup facility for offline printing. It might also be possible to substitute batch processing for online processing temporarily. In some cases, where compatible hardware is not available, it may be feasible to maintain a second software package which is functionally identical to the regular package but technically compatible with the offsite ADP hardware that is available for backup use.

3. Modify tasks to reduce run time. To stretch available backup resources, it might be feasible to eliminate or postpone portions of a task, such as information-only reports or file updates which are not time urgent. In some cases, it might help to double the cycle time for a task, that is, run a daily task every other day instead.

By considering all these possibilities for each task, the DP technical manager can develop the specifications for the minimum backup requirements (ADP hardware, resources, and hours per day) necessary for adequate backup.

To evaluate alternate backup modes and offsite facilities, the DP technical manager should consider such factors as:

1. ADP hardware usage.
2. Transportation of military and civil service personnel with needed supplies and materials.
3. Maintenance personnel at the offsite location.
4. Overtime cost factor for civil service personnel.

As these factors come into focus—identification of critical tasks, specific backup modes, and usable offsite ADP facilities—the outlines of the optimum backup plan will begin to emerge. In general, it is wise to form several COOP backup plans, for example:

1. A plan for backup operation which is not expected to extend much beyond the cause of delay which forces a shift to backup operation, viz., a minimum duration plan which would probably include only the most time urgent ADP tasks.

2. A plan for backup operation for as long as it takes to reconstruct the ADP facility after total destruction, or the worse case plan.

3. Plans for one or more operating periods between minimum duration and worst case.
4. A plan for each major partial failure mode.

While the individual COOP plans are geared to different objectives, they can usually be constructed from a common set of modules. It is often most effective to make a detailed plan for total destruction since this is the most demanding situation. Scaled-down versions or individual elements from this plan can then be used for the less demanding situations.

Each COOP backup plan should cover these five basic areas:

1. Performance specifications. This is a statement of the specific ways in which performance of each task departs from normal, e.g., tasks postponed, changes in cycle times, schedules, etc.

2. User instructions. Backup operation may require that users submit input in different forms or to different locations or may otherwise call for altered procedures. These should be clearly spelled out to avoid confusion and wasted motion.

3. Technical requirements for each ADP task. Backup operation of an ADP task will require the availability at the offsite ADP facility of the following: current program and data files, input data, data control and operating instruction (which may differ from normal instruction), preprinted forms, carriage control tapes, etc. These requirements must be documented for each task. Procedures also need to be established to ensure that the materials needed for backup operation are maintained offsite on a current basis.

4. Computer system specifications. One or more offsite computer systems are selected for backup operation. The following information should be recorded for each system: administrative information about the terms of backup use, the location of the system, the configuration and software operating system, a schedule of availability for backup operation, and the tentative schedule of ADP tasks to be performed on the system.

5. Administrative information. It is probable that COOP backup operation will require special personnel assignments and procedures, temporary employment or reassignment of personnel, use of special messengers, and other departures from normal. Details are to be documented along with guidance on obtaining required approvals.

When each of the COOP backup plans is completed, it should include full documentation and be approved by upper management. Each of the plans may have considerable duplication, but it is suggested that each plan be completely documented in order to be sure that nothing has been overlooked.

Recovery Planning

The use of a backup facility usually occasions both extra expense and downgraded performance. It is therefore worthwhile to give some thought to recovery and to develop and maintain supporting documents which minimize the time required for recovery. Furthermore, the ADP staff will be hard pressed by backup operations. If others can handle recovery, the workload on the ADP staff will be reduced during the emergency and the process will undoubtedly be carried out more effectively and economically. Recovery from total destruction requires that these tasks be completed:

1. Locate and obtain possession of enough floor space to house the ADP facility with a live load capacity as required by the ADP hardware and suitably located with respect to users and ADP staff spaces.

2. Perform required modifications for needed partitions, raised floor, electric power distribution, air conditioning, communications, security, fire safety, and any other special requirements.

3. Procure and install ADP hardware.

4. Procure needed supplies, office equipment and furniture, tape storage racks, decollators, etc.

5. Verify that all needed hardware, equipment, and materials are on hand and in good working order and then transfer operations from the backup site to the reconstituted ADP facility.

If the necessary documents have been prepared and stored offsite prior to the emergency, it should be possible for all but the last tasks to be completely reconstructed with minimum effort. Figure 3-12 shows a simplified step diagram of a normal reconstruction effort.

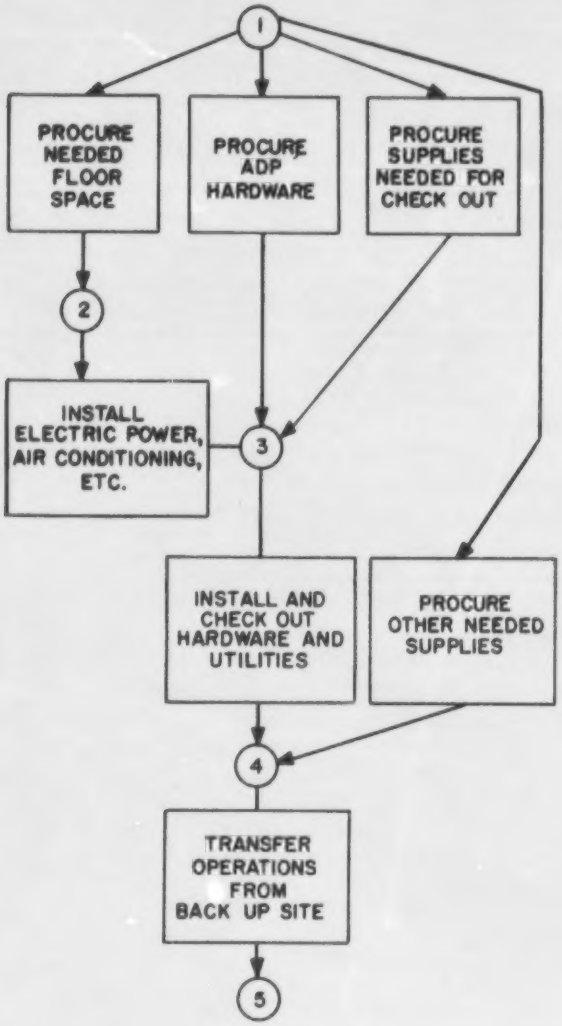


Figure 3-12.—Simplified diagram of ADP facility reconstruction.

COOP TESTING

Since emergencies do not occur often, it will be difficult to assure adequacy and proficiency of personnel and plans without regular training and testing. Therefore, it is important to plan and budget for both. The availability of needed backup files may be tested for by attempting to repeat a particular task using onsite hardware but drawing everything else from the offsite location. Experience has demonstrated the value of such tests in validating backup provisions; it is not uncommon to discover gross deficiencies despite the most careful planning. Compatibility with the offsite facility should be verified regularly by running one or more actual tasks. A number of ADP facilities conduct such tests as a part of an overall audit.

Similar tests of procedures for fire fighting, loss control, evacuation, bomb threat, and other emergencies will give assurance that plans are adequate and workable and will at the same time provide an opportunity for training of ADP personnel. Each test should have a specific objective. A team should be assembled to prepare a scenario for the test, to control and observe the test, and to evaluate the results. This evaluation provides guidance for modifications to emergency plans and for additional training. The important point is to be sure that the emergency plans have substance and do, in fact, contribute to the security of the ADP facility.

PHYSICAL SECURITY AUDITS

Every naval ADP facility should have an ADP physical security program and the final element of the program should be a review or audit process. The audit should be an independent and objective examination of the information system and its use (including organizational components) and include the following:

1. Checks to determine the adequacy of controls, levels of risks, exposures, and compliance with standards and procedures.

2. Checks to determine the adequacy and effectiveness of system controls versus

(dishonest, inefficiency, and security vulnerabilities.) The words "independent" and "objective" imply that the audit complements normal management inspections, visibility, and reporting systems and that it is neither a part of, nor a substitute for, any level of management.

What can an audit be expected to accomplish? First, it evaluates security controls for the ADP facility. Second, it provides each level of management an opportunity to improve and update its security program. Third, it provides the impetus to keep workers and management from becoming complacent. Fourth, if done effectively, it tends to uncover areas of vulnerability. Remember, risks change and new threats arise as systems mature.

Major factors to consider in determining the frequency of internal audits include the frequency of external audits, the rate of change of the ADP system, the amount and adequacy of controls, the threats that face the facility, the results of previous audits, and the directions of higher authority. Audit activity, direction, and implementation are usually at the discretion of the commanding officer of the command that has jurisdiction over the ADP facility.

AUDIT PREPARATION

One of the main principles in audit team selection is that members should not be responsible for ADP operations. This means that the audit should be conducted by some department or facility outside of the span of control of the DP technical manager. Team members should have some knowledge of data processing and, if possible, basic auditing principles. A programming or ADP operations background is desirable but not essential. An experienced military or civil service user of ADP services might have the necessary qualifications. The role of the team is not to develop security controls, but to evaluate established controls and procedures. Nor should it be responsible for the enforcement of control procedures, which is clearly an ADP management responsiblity.

The character of each of the audit team members is extremely important. Judgment, objectivity, maturity, ability, and a probing nature will all affect the success of the audit. The leader of the audit team must be able to organize the efforts, prepare a good written report, communicate findings effectively, be an officer, warrant officer, chief petty officer, or U.S. civilian employee GS-7 or above. If not technically oriented, the team leader should be assisted by someone whose technical judgment and knowledge of ADP is reliable.

The size of the team depends upon the size of the installation and the scope of the audit. A large installation should consider including personnel from the following areas on the audit team:

1. Internal audit. The knowledge and discipline to conduct an audit can be provided through internal audit specialists. Inquisitiveness, a probing nature, and attention to detail are typical characteristics desired for audit board members. Even though an auditing team member generally is not trained in data processing technology, it should not be difficult to appoint team members with some data processing knowledge.

2. Security. Each audit team is appointed in accordance with OPNAVINST 5510.1 series. A security officer is a welcome addition to an audit team.

3. Data processing. Technical expertise in data processing is required. Both programming knowledge and operations experience is helpful. Perhaps the data processing internal security officer has these skills, and if so, should be a prime candidate for the team. Using someone from the ADP facility that is being evaluated need not significantly affect the objectivity of the audit process.

4. Users. Users have the most tó gain from an effective audit because of their dependence on the ADP facility, yet too often they have little or no interest in ADP controls or security measures. To encourage participation in the ADP security program, one or more users who are concerned about sensitive data being compromised, disclosed, or destroyed should be motivated to join or should be appointed to the audit team.

5. Building management. Many of the physical security controls to be audited—fire prevention and detection, air conditioning, electric power, access controls, and disaster prevention—relate to building management and engineering.

6. Outside specialists. Independent, experienced viewpoints provided by outside consultants can be very helpful.

The composition of the team can be flexible. One of the prime requirements is that it consist of people who are objective. If only one ADP facility is to be audited, the members of the team can be assigned for the term of the audit and then returned to their normal jobs. If there are many ADP facilities under the jurisdiction of the command, it might be advisable to establish a permanent audit team to review all installations on a recurring basis. In any event, the composition of the team should be changed periodically in order to bring in fresh viewpoints and new and different audit techniques.

THE AUDIT PLAN

In order to properly conduct an internal audit of security, a comprehensive audit plan must be developed. It should be action-oriented, listing actions to be performed. It must be tailored to the particular installation. This means that quite a bit of work is required in its development.

The first step is to examine the security policy for the ADP facility. This policy may apply to an entire Naval district, a command, a ship, department, or a single ADP facility. In any case, it should be reviewed and pertinent security objectives extracted for subsequent investigation. The next step is to review the risk analysis plan, identifying those vulnerabilities that are signficant for the particular installation. Third, the ADP Facility Security Manual, the Operations Manual, and other such documents should be reviewed in order to determine what the specified security operating procedures are. And last, the ADP facility organization chart and job descriptions should be examined to identify positions with specific security or internal control responsibilities. This background material forms the basis for the development of the audit plan. There are a number of general questions that should be considered when formulating the audit program:

1. What are the critical issues with regard to security? Does the ADP facility process classified or otherwise sensitive data? Does the processing duplicate that of other data centers, thereby providing some sort of backup or contingency capability, or is it a stand-alone activity processing unique applications? What are the critical applications? What are the critical applications in terms of the audit emphasis?

2. What measures are least tested in day-to-day operations? For example, if the computer fails every day at 1615 because of power switchovers, the immediate backup and recovery requirements are likely to be well formulated and tested. However, the complete disaster recovery plan probably has not been tested, unless there is a specific policy to do so. This is a key point. Security measures of this type are often inadequately exercised.

3. What audit activities produce the maximum results for least effort? A test of fire detection sensors under surprise conditions tests not only the response to alarms but also the reaction of the fire party and the effectiveness of evacuation plans. In interviewing personnel, questions should be designed to elicit comprehensive answers. For example, the question "How would you run an unauthorized job?" is likely to elicit more information than "Are job authorization controls effective?" The most likely answer to the second question is a simple and uninformative "Yes."

4. What are the security priorities? Because of particular policy, a request for an investigation, or an incident of loss, interruption or compromise, the testing of a particular security measure probably should receive more emphasis than another equally important but noncurrent topic. One must, however, avoid irrational concentration on any one aspect of the program. Management overemphasis as a result of a recent security breach should be tempered with a rational approach toward investigating all aspects of computer security.

Another step in the process of developing an audit plan is the review of previous audit reports. Many times these identify weaknesses or concerns which should have been corrected, and so should be an item of special attention in the current audit.

CONDUCTING AUDITS

There are advantages to be gained from using both scheduled and surprise audits. A scheduled audit should meet the general policy requirements of the particular installation and should occur at least annually. This could be a major audit conducted by an outside command, an internal audit, or a spot check audit to review specialized items of interest, perhaps as a result of previous audit reports of findings. The distinguishing characteristic is that it is scheduled in advance, with a resultant flurry of preparation by the data centers. It motivates cleaning up loose ends, but limits what can really be learned from the audit. A surprise audit, should be approved by the Commanding Officer of the command in charge of the ADP facility and is designed to test on a no-notice basis certain elements of security and control. It can be accomplished by the command or an external audit team, and it can be used to test those elements best reviewed on a surprise basis, such as fire response, access control, and personnel complacency.

In conducting an audit, the first step normally is to interview ADP personnel, although this is not the case if any surprise tests were required. Generally, the first walk-through includes interviews with the data processing technical manager. Searching, rather than leading questions should be the rule, and the best approach is to allow the interviewee to talk as freely as possible. Ask questions to put the interviewees in the position of probing for their answers. For example, "What is your biggest access control problem?" not "Do your people wear badges?" Ask how illegal entry or sabotage would be accomplished. Do not hesitate to ask the same questions of more than one person. It is interesting how varied the responses can be. The conduct of the interviewer is important. Strive to be open in dealing with interviewees and avoid allusions to private information and obscure references to other people or events or in any other way cultivating an air of mystery or superiority. It goes without saying that the use of good human relations techniques is essential to a successful interview. Nothing can be gained by being belligerent and antagonizing the interviewee. Your conduct should be firm and inquisitive but also calm, sincere, and open. Any answer which appears evasive or defensive should be probed in some detail.

The taking of notes is a matter of individual preference. Some individuals take very adequate notes at listening speed. Others must devote all their attention to listening. If note taking is a problem, the interview could be conducted by two-person teams. Another alternative is to use a portable tape recorder, making certain that the subject knows in advance that the interview is being taped. If none of the above is possible, you should attempt to listen and absorb as much as possible, then record notes and impressions directly after the conclusion of the interview.

The evaluation tests can be scheduled or come as a surprise. Most security audits include a testing of the emergency, fire, evacuation, and disaster recovery activities. Access controls should also be tested on a no-notice basis. Tests are best scheduled or conducted early in the audit rather than after everyone is alerted to the presence of the audit team. Special concern, guidance, and instructions must be taken into consideration when the ADP facility has armed guards. It is possible to test the adequacy of programmed controls and data authorization by submitting jobs that attempt to bypass these controls. Care must be taken not to destroy live data. However, if ADP upper management believes that error detection and correction controls really work, then there should be no objection to the introduction of deliberate errors to test these controls.

The audit team should convene periodically, preferably at the end of each day's activity, to review progress and to compare notes. Areas of weakness or concern should be highlighted, and additional tests or interviews scheduled to investigate further any particular areas of concern. Copies of the audit working paper should be classified, numbered, dated and

organized for ease of understanding, review, and comparison.

At the completion of the audit, a written report is to be prepared immediately, while impressions are still fresh. As a rule the audit report includes:

1. An executive summary
2. A description of the audit–dates, locations, scope, objectives, etc.
3. A detailed report of observations made
4. Conclusions drawn from the observations
5. Recommendations for corrective actions, as appropriate

The degree of cooperation recieved should be noted and favorable conclusions should be given the same prominence as deficiencies. Tables, charts, and matrices of results, statistical tests, and conclusions may be very helpful. In the planning phase, agreement should be reached as to how the final report is to be distributed to the ADP facility and command's upper management.

AUDIT FOLLOW-UP

An audit is of little use unless it is the basis for improvement, correction, and management follow-up. The responsibility for implementation of such activity normally resides with the Commanding Officer (CO) of the command. The CO must, in turn, assign responsibilities for corrective action. The best approach is to summarize each major deficiency on a control sheet, outlining requirements, problem definition, responsibility, action taken or required, and follow-up action. In addition, an indication should be made of the date that action should be completed, or if it is to continue. Some of the corrective action may require additional funds and this should be noted.

Corrective action, follow-up, and disposition of the deficiencies should follow a recurring reporting cycle to upper management. Quarterly reports are recommended for any audit control items still open.

The final step is a frank and honest evaluation of the audit itself by ADP facility management and the audit team. A group discussion should be held with the expressed purpose of improving future audit procedures and process. The audit plan may be amended as needed or the team composition may need to be changed. The emphasis of the audit should always be positive–one of helping ADP management at all levels to improve the security and control of the ADP facility.

DATA PRIVACY

The Privacy Act of 1974 (Public Law 93-579) imposes numerous requirements upon naval commands to prevent the misuse or compromise of data concerning individuals. Navy ADP facilities which process personnel data must provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of personnel data, whether it is intentional or results from an accident or carelessness.

SECNAVINST 5239.1 series provides guidelines for use by all Navy organizations in implementing any security safeguards which they must adopt in order to implement the Privacy Act. It describes risks and risk assessment, physical security measures, appropriate information management practices, and computer system/network security controls.

SECNAVINST 5211.5 series implements the Privacy Act and personal privacy and rights of individuals regarding their personal records by delineating and prescribing policies, conditions, and procedures for the following:

1. Any Department of the Navy system of records possessing a record on an individual must verify it has the record upon the request of the individual.

2. The identity of any individual requesting personal record information maintained on them must be confirmed before the information is released.

3. An individual must be granted access to their personal files on request.

4. Any request from an individual concerning the amendment of any record or information pertaining to the individual for the purpose of making a determination on the request or appealing an initial adverse determination must be reviewed.

5. Personal information is collected, safeguarded, and maintained, and decisions are made concerning its use and dissemination.

6. The disclosure of personal information, and decisions concerning which systems of records are to be exempted from the Privacy Act.

7. Rules of conduct are established for the guidance of Department of the Navy personnel who are subject to criminal penalties for noncompliance with the Privacy Act.

The Chief of Naval Operations (OP-09B) is responsible for administering and supervising the execution of the Privacy Act and SECNAVINST 5211.5 series within the Department of the Navy. Additionally, the Chief of Naval Operations (OP-09B1) is designated as the principal Privacy Act coordinator for the Department of the Navy.

The major provisions of the Privacy Act which most directly involve computer security are found in the following parts of title 5, United States Code (U.S.C.), section 552a:

1. Subsection (b)–limits disclosure of personal information to authorized persons and commands.

2. Subsection (e)(5)–requires accuracy, relevance, timeliness, and completeness of records.

3. Subsection (e)(10)–requires the use of safeguards to ensure the confidentiality and security of records.

Although the Privacy Act sets up legislative prohibitions against abuses, technical and related procedural safeguards are required in order to establish a reasonable confidence that compliance is indeed achieved. It is therefore necessary to provide a reasonable degree of protection against unauthorized disclosure, destruction, or modification of personal data, whether it is intentional or results from an accident or carelessness.

The following terminology is used throughout the remainder of this chapter in discussing the treatment of "personal data":

1. Confidentiality–A concept which applies to data. It is the status accorded to data which requires protection from unauthorized disclosure.

2. Data Integrity–The state existing when data agrees with the source from which it is derived, and when it has not been either accidentally or maliciously altered, disclosed, or destroyed.

3. Data Security–The protection of data from accidental or intentional, but unauthorized, modification, destruction, or disclosure.

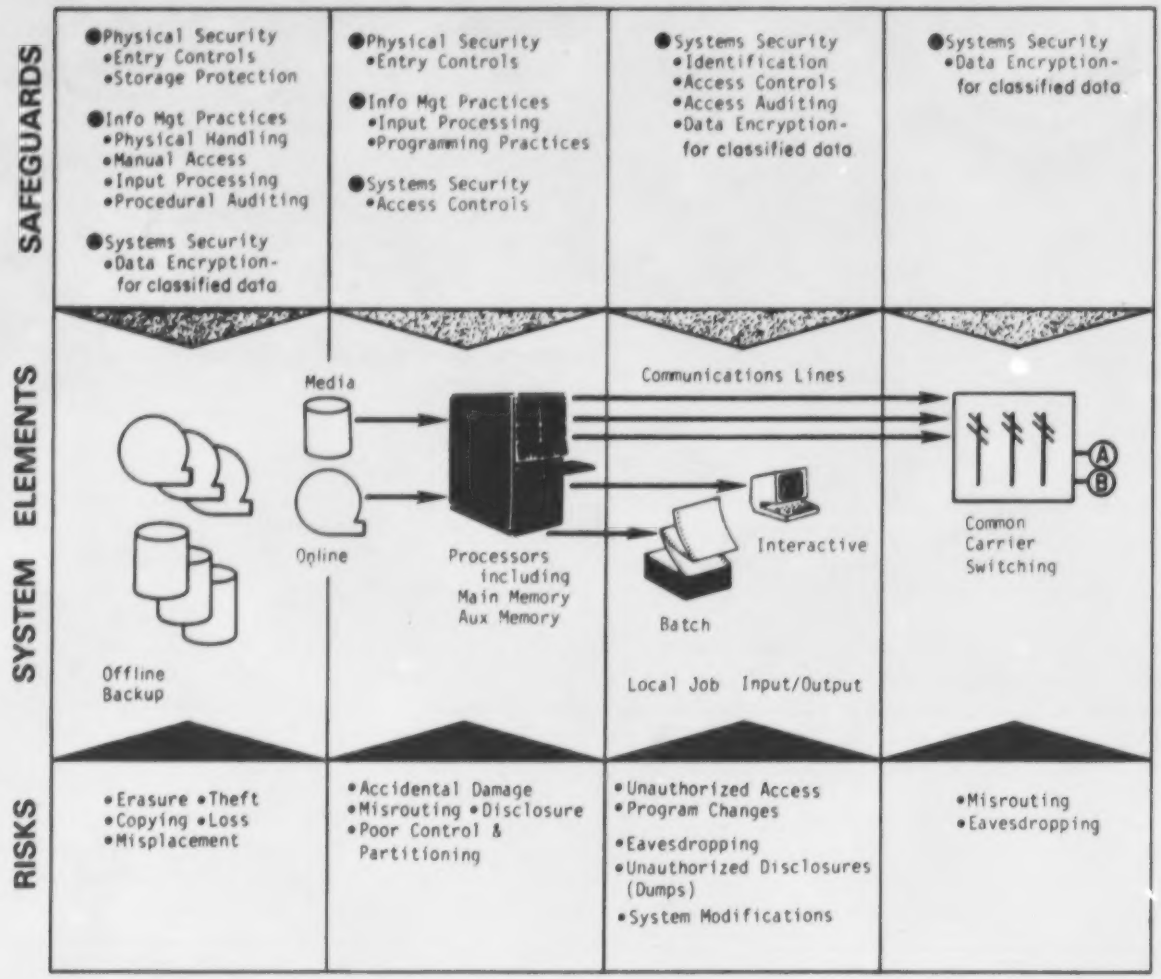
Safeguards which provide data protection are grouped into three categories: physical security measures, information management practices, and computer system/network security controls. Specifically, these are:

1. Physical Security Measures–Measures for protecting the physical assets of a system and related facilities against environmental hazards or deliberate actions as discussed earlier in this chapter.

2. Information Management Practices–Procedures for collecting, validating, processing, controlling, and distributing data.

3. Computer System/Network Security Controls–Techniques available in the hardware and software of a computer system or network for controlling the processing of and access to data and other assets.

Since the present emphasis is on "personal data," the term "data" will be used



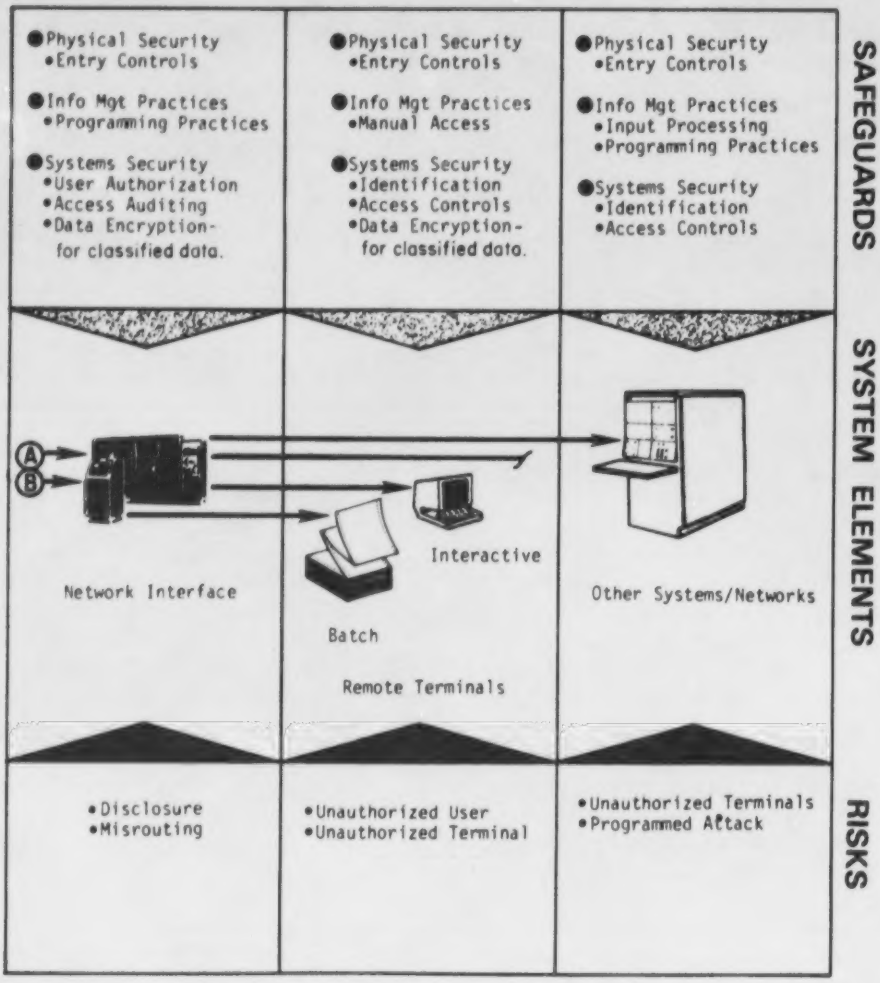
synonymously with "personal data" for the remainder of this chapter.

Technological safeguards are presented in figure 3-13, where they may be viewed in relation to the control points within a computer system/network where security risks occur and where appropriate safeguards can be applied. This perspective shows the elements of a computer network, beginning with the offline storage of data in machine-readable media (e.g., tapes and disks) and progressing through the many possible processing modes. It includes the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses the value of physical security measures and information management practices, in relation to computer system/network controls.

DATA RISK ASSESSMENT

The first step toward improving a system's security is to determine its security risks using the criteria discussed earlier in this chapter. A data security risk assessment benefits a command in three ways.

1. It provides a basis for deciding whether additional security safeguards are needed for data.



78.169

Figure 3-13.–Technological safeguards and data security risks.

2. It ensures that additional security safeguards help to counter all the serious data security risks.

3. It saves money that might have been wasted on safeguards which do not significantly lower the overall data risks and exposures.

The goal of a risk assessment is to identify and prioritize those events which would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event and its probability of occurrence.

In general, the risk assessment should consider all risks, not just risks to personal data. While this section of the chapter emphasizes the security of personal data, it is best to develop an integrated set of security safeguards and requirements which protect all classified and other valuable data in the system wherever possible.

The risk assessment should be conducted by a team which is fully familiar with the problems

that occur in the daily handling and processing of the information. The participants on the risk assessment team should include experienced representatives from:

1. The operating facility supported by or having jurisdiction over the data under consideration
2. The programmers responsible for support of the operation or function under consideration
3. The facility responsible for managing ADP operations
4. The system programmers–if the command has this as a separate function
5. The DP assigned the responsibility for overseeing or auditing system security
6. Those responsible for physical security

DATA SECURITY RISKS

Each command should identify its specific risks and evaluate the impact of those risks in terms of its information files. Experience indicates that the most commonly encountered security risks are usually accidents, errors, and omissions. The damage from these accidental events far exceed the damage from all other data security risks. Good information management practices are necessary to reduce the damage that can result from these occurrences. Some data security risks include:

1. Input error–Data may not be checked for consistency and reasonableness at the time they are entered into the system: or data may be disclosed, modified, lost, or misidentified during input processing.

2. Program errors–Programs can contain many undetected errors–especially when they are written with poor programming practices or are not extensively tested. A program error may result in undesirable modification, disclosure, or destruction of sensitive information.

3. Mistaken processing of data–Processing requests may update the wrong data; for example, if a tape is mounted at the wrong time.

4. Data loss–Data on paper printouts, magnetic tapes, or other removable storage media may be lost, misplaced, or destroyed.

5. Improper data dissemination–Disseminated data may be misrouted or mislabeled, or it may contain unexpected personal information.

6. Careless disposal–Personal data can be retrieved from waste paper baskets, magnetic tapes, or discarded files.

Every ADP facility's DP technical manager and upper management should establish strict controls and procedures over individuals authorized to access the personnel data files. If everyone at the facility needs authority to access personal data files, the physical security measures should adequately control system access. If there are persons working on the system who are limited in their access, the following risks should be considered:

1. Open system access–There may be no control over who can either use the ADP system or enter the computer room.

2. Theft of data–Personal data may be stolen from the computer room or other places where it is stored.

3. Unprotected files–Data files may not be protected from unauthorized access by other users of the ADP system. This applies to online files and also to offline files such as magnetic tapes. The latter are sometimes accessible simply by requesting that they be mounted.

4. Dial-in access–There is serious danger that unauthorized persons can access the system when remote, dial-in access is allowed.

5. Open access during abnormal circumstances–Data which is adequately protected during normal operations may not be adequately protected under abnormal circumstances. Abnormal circumstances include power failures, bomb threats, and natural disasters such as fire or flood.

Physical destruction or disabling of the ADP system is not normally a primary risk to privacy. All computer systems presently in use are vulnerable to deliberate penetrations which can bypass security controls. These types of security penetrations require vast amounts of technical knowledge. At present, the Navy has very few instances of these types of actions. Commands

that are designing large computer networks should consider the following risks in the early planning stage:

1. Misidentified access–Passwords are often used to control access to a computer or to data, but they are notoriously easy to obtain if their use is not carefully controlled. Furthermore, a person may use an already logged-in terminal which the authorized user has left unattended, or may capture a communications port as an authorized user attempts to disconnect from it.
2. Operating system flaws–Design and implementation errors in operating systems allow a user to gain control of the system. Once the user is in control. the auditing controls can be disabled, the audit trails erased, and any information on the system accessed.
3. Subverting programs–Programs containing hidden subprograms that disable security protections can be submitted. Other programs can copy personal files into existing or misidentified files to use when protection is relaxed.
4. Spoofing–Actions can be taken to mislead system personnel or the system software into performing an operation that appears normal but actually results in unauthorized access.
5. Eavesdropping–Communications lines can be "monitored" by unauthorized terminals to obtain or modify information or to gain unauthorized access to an ADP system.

INFORMATION MANAGEMENT PRACTICES

Information management practices refer to those techniques and procedures used to control the many operations performed on information to accomplish the command's objectives, but do not extend to the essential managerial determination of the need for and uses of information in relation to any command's mission. In this context, information management includes: data collection, validation and transformation; information processing or handling; record keeping; information control, display, and presentation; and, finally, standardization of information management operations.

It is suggested that changes to current practices be analyzed by the DP technical manager prior to enacting new policies in personal data handling procedures. The information management guidelines presented in the following material are grouped into major categories to facilitate the explanation of their role. Every practice presented may not be required at every Navy ADP facility by upper management. The DP technical manager should select only the suggested practices that are relevant to the designated command's environment and mission, or approved by upper management.

Handling of Personal Data

Access to personal information shall be limited to authorized individuals of agencies in the Department of Defense who have an official need for the record, except when the information is otherwise releasable under the disclosure or access provisions of the Privacy Act.

The following practices are suggested for the handling of personal data.

1. Prepare a procedures handbook which describes the precautions to be used and obligations of computer facility personnel during the physical handling of all personal data. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act. Personal information that is processed, accessed, maintained, or disposed of by contractors shall be handled within the terms and conditions of Section 7-104.96 of the Defense Acquisition Regulation.
2. Label all recording media which contain personal data. Labeling such media reduces the probability of accidental abuse of such data, and also aids in fixing the blame in the event of negligent or willfully malicious abuse. If the information resides on removable storage media, it should be externally labeled. External warnings shall clearly indicate that the media contain personal information subject to the Privacy Act; e.g. PERSONAL DATA–PRIVACY ACT of 1974. It should be noted that abbreviations must not be used.

3. Store personal data in a manner that conditions users to respect its confidentiality; e.g., under lock and key when not being used.

4. If a program generates reports containing personal data, have the program print clear warnings of the presence of such data on the reports.

5. Color code all computer input/output card trays, tape reels, disk pack covers, etc., which contain personal data, so that they can be afforded the special protection required by law.

6. Keep a record of all categories of personal data contained in computer-generated reports to facilitate compliance with the requirements that each command identify all such data files and their routine use by the command.

7. Carefully control products of intermediate processing steps, e.g., scratch tapes and disk packs, to ensure that they do not contribute to unauthorized disclosure of personal data.

8. Maintain an up-to-date hard copy authorization list of all individuals (computer personnel as well as system users) allowed to access personal data for use in access control and authorization validation.

9. Maintain an up-to-date hard copy data dictionary listing the complete inventory of personal data files within the computer facility in order to account for all obligations and risks.

Maintenance of Records to Trace the Disposition of Personal Data

The following practices are suggested for the maintenance of records.

1. Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility.

2. Log each transfer of storage media containing personal data to or from the computer facility.

3. Maintain logbooks for terminals that are used to access personal data by system users.

Data Processing Practices

The following practices are suggested for data processing procedures.

1. Use control numbers to account for personal data upon receipt and during input, storage, and processing.

2. Verify the accuracy of the personal data acquisition and entry methods employed.

3. Take both regular and unscheduled inventories of all tape and disk storage media to ensure accurate accounting for all personal data.

4. Use carefully devised backup procedures for personal data. A copy of the data should be kept at a second location if its maintenance is required by law.

5. Create a records retention timetable covering all personal data and stating minimally the data type, the retention period, and the authority responsible for making the retention decision.

6. After a computer failure, check all personal data which was being processed at the time of failure for inaccuracies resulting from the failure.

7. If the data volumes permit economic processing, some sensitive applications may use a dedicated processing period.

8. Files created from files known to contain personal data should be examined to ensure that they cannot be used to regenerate any personal data. A formal process must be established for the determination and certification that such files are releasable in any given instance.

9. In aggregating data, give consideration to whether the consequent file has been increased in value to a theft-attracting level.

10. When manipulating aggregations and combinations of personal data, make it impossible to trace any information concerning an individual. Steps should be taken so that no inference, deduction, or derivation processes can be used to recover personal data.

Programming Practices

The following practices are suggested for programming procedures.

1. Subject all programming development and modification to independent checking by a second programmer, bound by procedural requirements developed by a responsible supervisor.
2. Inventory current programs which process or access personal data; verify their authorized usage.
3. Enforce programming practices which clearly and fully identify personal data in any computer program.
4. Strictly control and require written authorization for all operating system changes that involve software security.

Assignment of Responsibilities

The following practices are suggested for the assignment of responsibilities.

1. Make a designated individual responsible for examining installation practices in the storage, use, and processing of personal data, including the use of physical security measures, information management practices, and computer system access controls. Both internal uses and the authorized external transfer of data should be considered by this individual and any risks reported to the relevant upper management authority and the DP technical manager.
2. Make a designated individual responsible during each processing period (shift) for ensuring that the facility is adequately manned with competent personnel and that the policies for the protection of personal data are enforced.
3. Ensure that all military, civil service, and other employees engaged in the handling or processing of personal data adhere to established codes of conduct.

Procedural Auditing

Whenever appropriate, conduct an independent examination of established procedures. Audits of both specific information flow and general practices are possible. The following points should be considered when developing an audit.

1. Auditing groups can be established within organizations to provide assurance of compliance independent of those directly responsible.
2. Independent, outside auditors can be contacted to provide similar assurance at irregular intervals.
3. Audit reports should be maintained for routine inspection and used to provide additional data for tracing compromises of confidentiality.

IDENTIFICATION TECHNIQUES

Once physical security measures and information management practices have been established, the DP technical manager should consider methods of personal identification of individuals for authorized access to the ADP facility. The identification of each individual who is allowed to use a system is a necessary step in safeguarding the data contained in that system.

For a broader knowledge of personal identification and identification techniques, refer to FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.

Security of all types should be a continuous matter with every DP technical manager. This chapter has scratched only the surface of the material available on classified security, physical security, and security and privacy. It is a subject with which every DP should be completely up to date. The material presented and referenced in this chapter should be studied for advancement in rate exams through the E7 level.

CHAPTER 4

SYSTEMS ANALYSIS

This chapter deals with a subject considered controversial by many knowledgeable ADP personnel. The dimension of the term "systems" and its unrestrained use have caused confusion about the term "systems analysis." The confusion has come from the fact that the term is not restricted to the data processor's community and terminology. It is used by economists, engineers, scientists, and many others. To make the situation worse, such terms as systems approach, systems applications, systems engineering, systems science, systems concepts and systems methods denote similar procedures and are sometimes used interchangeably with the term systems analysis.

The term "analysis" is defined in the American National Dictionary for Information Processing (FIPS PUB 11-1) as "The methodical investigation of a problem, and the separation of the problem into smaller related units for further detailed study." The term "systems analysis" is defined in the ADP Glossary (NAVSO P-3097) as (1) "The examination of an activity, procedure, method, technique, or business to determine what must be accomplished and how the necessary operations may best be accomplished. (2) To conduct an orderly study of the detailed procedures of collecting, organizing, and evaluating the data of a system."

It is not the intent of this chapter to set policy, standards, or procedure for any ADP installation. The purpose of this chapter is to aid the DP2 in becoming knowledgeable of the requirements, functions, and general performances and tasks of an analyst. However, this chapter gives only short simulated problem situations because of text limitations.

Many factors prevent the formulation of exact rules, standards, and instructions for systems analysts to follow. Some of these factors are:

1. The variety of different data processing systems that the Navy maintains.
2. The volume of manuals that would be required to describe these data processing systems.
3. The different configuration of each of these systems.
4. The different requirements of each command supported by each of the ADP facilities.

There are many avenues of approach that an analyst can take when collecting, organizing, and evaluating facts about a system problem and the environment in which it operates. These avenues of approach, including the design and implementation of problem solutions, assist management in their decisions. The main objective of a systems analysis is to learn enough about a problem either to establish the foundation for designing and implementing a new system to solve the problem, remedy or to correct the present system if it is found desirable or feasible to do so. The majority of the Navy DP analyst's functions will involve investigating problems, designing new procedures, and recommending actions needed to fully utilize a command's present computer system.

DEFINITIONS

To reduce the possibility of confusion and enhance the understanding of the terminology

used in the area of systems analysis, the following definitions and terms as used in this chapter are emphasized:

1. Systems Analyst.–A systems analyst investigates problems and develops algorithms and procedures for their solution in ALL areas of data processing. This person should have an extensive knowledge of and background experience in operations, programming of COBOL and FORTRAN, data management and information collection, leadership, and management experience.

2. Problem Analyst.–A problem analyst investigates problems and develops procedures for their solution. This person should have an extensive knowledge of and background experience in operations and ADP management, and the ability to converse with all ADP management, and the ability to converse with all ADP area personnel, and management. This person should have an excellent ability to speak, read, write, and understand ADP-oriented terminology.

3. Data Analyst.–A data analyst investigates problems and develops procedures for their solution. This person should have an extensive knowledge of and background experience in managing a Data Base Management System, organizing data and files, as a Data Base Administrator (DBA), creating and formatting reports, and writing systems utilities. This person should also display leadership qualities and be thoroughly conversant in ADP management problem-solving techniques.

4. Programming Analyst.–A programming analyst investigates problems and develops procedures for their solution. This person should have an extensive knowledge of and background experience in programming, COBOL, FORTRAN, the parent systems Assembler Language Coding (ALC), and other high and low level languages appropriate for the parent system. This person should have the ability to document all requirements of the particular system concerned in accordance with SECNAVINST 5233.1 series, revise software requirements, debug all parent system software, interpret core dumps, and write subroutines. This person should also be knowledgeable in segmentation, overlays, parent systems software procedures, and job control language.

5. Design Analyst.–A design analyst creates and develops procedures for problem solution. This person should have an extensive knowledge of and background experience in operations and programming management. This person should also have extensive knowledge of hardware and software capabilities and the ability to solve complex problems of hardware and software interfacing.

6. Systems Study Plan.–A systems study plan is the broad framework of objectives that management has set forth for the analyst to follow when conducting a systems analysis for a single problem or a complete system. A system study plan gives the guidelines required by upper management to determine the facts and establish minimum requirements to efficiently complete the analysis. Further, it gives detailed instructions on how the analysis is to be conducted and suggestions for the analyst to follow.

7. Systems Design.–A systems design is the development of a plan or scheme for processing data based on the facts gathered in the systems analysis. It is done within the framework developed during the design phase of the systems analysis (study). Systems design can be in the area of redesigning software or hardware for the parent computer; meeting a new software or a new hardware requirement; or designing and putting together a complete new system to meet the requirement of upper management.

8. Feasibility study.–A feasibility and economic analysis is conducted for a total systems analysis and is generated by higher authority in accordance with SECNAVINST 5231.1 series.

THE SYSTEMS ANALYST

All Navy ADP facilities, regardless of size, have some type of task analysis to perform. The data processing department must develop and maintain a series of computer programs in order to meet information requirements and accomplish the ADP facility's mission.

JOB DESCRIPTION

In the Navy Enlisted Classification Codes Manual (NEC-2751) a systems analyst billet description is as follows:

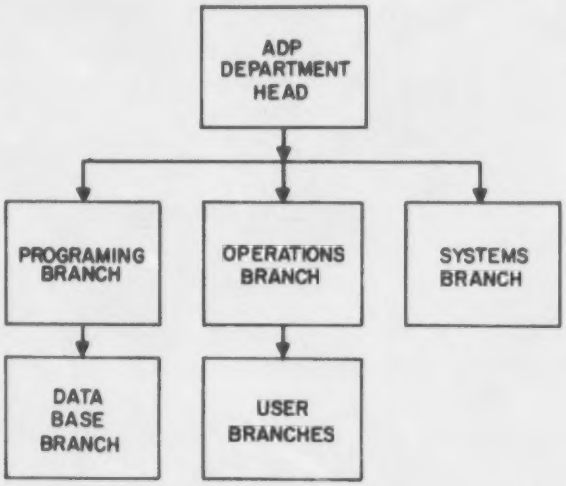
> "Subdivides given problems into their simplest parts. Coordinates with system sponsor selection of essential elements, including determination of their relationships, and designs necessary procedures to achieve the desired results. Performs job analysis, Program Evaluation Review Technique (PERT) and Critical Path Method (CPM) analyses and designs software procedures. Performs document analysis simulation and design."

To obtain the DP-2751 systems analyst NEC requires 6 months of experience as a systems analyst on any computer system other than the Honeywell H6000 series.

Have you ever asked more than one person the question, "What is a systems analyst and what is his/her function within the data processing organization?" More than likely their responses were totally different. While a great deal has been written about the overall ADP organization and the data processing system which supports the organization, very little has been written in the DP's rate training manual about the data processing systems analyst. The reasons for this are as varied as the answers that you would receive to the question, "If I had a systems analyst NEC, what would be my job at a large ADP facility?" The major reason for this is that the data processing department of any single organization is likely to differ considerably in structure, equipment used, and configuration from that of any other organization. Additionally, the missions of the commands that the ADP facilities support are different.

The three common principal functions performed within a data processing department usually result in the basic configuration shown in figure 4-1.

A systems analyst can be compared to a handyman or a person who is known as a "jack-of-all-trades." Their duties and



78.147

Figure 4-1.–Typical organization of an ADP department.

responsibilities will vary at each new command or billet. The systems analyst is a member of the Systems Analysis and Design Branch at most Navy ADP facilities. The position or billet that an analyst occupies may be responsible for the following duties:

1. Serve on project teams and perform duties as required in developing and documenting the concepts, principles, and specifics applicable to designing the procedure for automatic data processing of information.

2. Analyze and evaluate ADP requirements for functional support for total systems applications.

3. Analyze hardware interfaces, software interfaces, communications interfaces, and time-sharing schemes as required.

4. Prepare questionnaires and conduct interviews.

5. Prepare reports, documentation, and charts, and collate reports for final review.

6. Report orally the progress or results of a systems analysis study to the users or upper management.

7. Attend planning, scheduling, and technical conferences on subjects relating to

ADP support of requirements for intelligence, management, and logistics functions.

8. Assist the users in defining information requirements.

9. Analyze and determine if available data can be transferred into information.

10. Evaluate available technology for use in problem solutions.

11. Evaluate and suggest the best mixture of resources (personnel, money, machines, material, and procedures) for implementing a new system (hardware or software).

12. Evaluate and determine parent system software flows, debug system errors, and recommend corrective procedures.

13. Analyze and design additional requirements for software and hardware for parent computer systems.

In general, the systems analyst analyzes the problems of the operations branch, programming branch, data base branch, and users branch. The systems analyst is the INTERFACE between all the branches of an ADP facility. This function is logical as well as important, because information systems are developed to fill the information requirements of a wide variety of users throughout a command. The systems analyst (or group of analysts) interface ensures that the system meets the users needs, while the programmers, operators, and data base administrators deal with the technical portions of the existing system.

EXPERIENCE

When detailing the background that a successful systems analyst should possess, a number of factors emerge. A formal education in ADP is not required to receive a 2751 NEC, nor does its possession guarantee to produce a good systems analyst. However, a college degree in either business or computer science does indicate that the individual has been exposed to modern business concepts and problem-solving techniques.

Before an individual considers applying for an analyst 2751 NEC, a self-evaluation covering past experience and background knowledge of analysis should be completed. Following are some guidelines that need to be considered in such an evaluation.

1. A government-sponsored manufacturer's analysis course should be completed successfully on the parent computer system or its equivalent, locally.

2. Experience should include:

a. At least 6 months operating the parent computer system.

b. At least 6 months programming the parent computer system using all programming languages inherent to the system.

c. At least 6 months as a Data Base Administrator on the parent computer system.

d. At least 6 months as an ADP manager, dealing with people effectively and harmoniously.

e. At least 6 months working with systems concepts and in data processing in general, becoming thoroughly familiar with the parent computer systems hardware and software capabilities.

f. At least 6 months working with documentation, becoming thoroughly familiar with all SECNAV instructions.

g. At least 6 months flowcharting problems on the parent computer system.

3. A formal education, including a college degree in business or computer science should be completed.

4. The desire to become a successful and completely qualified systems analyst should be expressed.

A qualified systems analyst should possess most of the preceding attributes and background experience. It would be difficult to find a person with less than 6 years experience in data processing with all of the preceding background experience. If the preceding list of qualifications were required rather than suggested, the Navy would have very few systems analysts. In actuality, an individual is granted an analyst NEC after 6 months of experience of any kind and gains background experience while functioning as an analyst in a specialized portion

of the analyst area of responsibility. Although officially a systems analyst once a 2751 NEC is received, some commands assign an individual with minimum experience to such locally titled billets as problem analyst, data analyst, programming analyst, or design analyst. The decision depends on the individual's background and experience (as defined earlier in this chapter). Take, for instance, an individual who has had extensive experience in programming and is thoroughly knowledgeable in the systems software, but has no operations experience or possesses limited knowledge of systems hardware capabilities. This individual would probably perform a very good analysis of a problem with software and perform poorly in analysis of a hardware-oriented problem. Naturally, this systems analyst should be assigned to a systems study team as a programming analyst and assist a problem analyst, thus gaining experience in the hardware area. Although all analysts with 2751 NECs are officially systems analysts, the local command progression, as related to experience and background on a particular computer system, is depicted in figure 4-2.

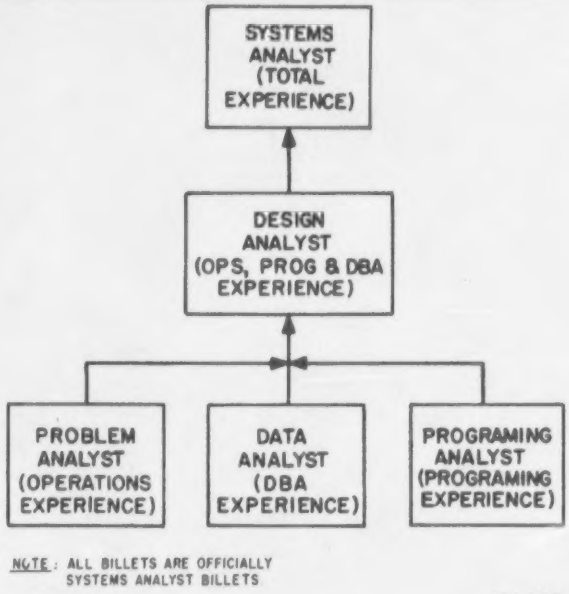

SYSTEMS ANALYST (TOTAL EXPERIENCE)
DESIGN ANALYST (OPS, PROG & DBA EXPERIENCE)
PROBLEM ANALYST (OPERATIONS EXPERIENCE)
DATA ANALYST (DBA EXPERIENCE)
PROGRAMING ANALYST (PROGRAMING EXPERIENCE)
NOTE: ALL BILLETS ARE OFFICIALLY SYSTEMS ANALYST BILLETS
78.148

Figure 4-2.—Common local command billet titles for systems analysts as related to background experience.

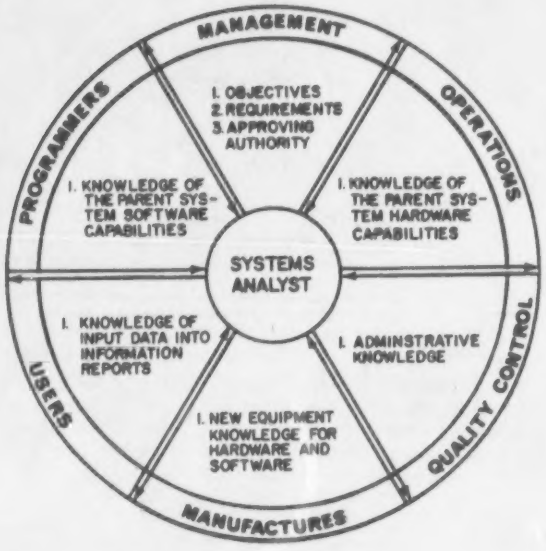
The lack of knowledge and experience in the areas of operations, data base creation and manipulation, and programming by a systems analyst may result in a new design or redesign of systems that are impractical from an operating, programming, and implementation standpoint. Generally speaking, a systems analyst should have more experience in ADP than an operator or programmer before becoming a successful DP-2751 systems analyst. To be a qualified and successful systems analyst takes time and experience. It does NOT come with the completion of this correspondence course or with the ability to speak ADP jargon and terminology. The cold and hard fact remains that a systems analyst must be skilled in the art and science of ADP problem solving.

INTERPERSONAL SKILLS

Next to experience, dealing with people effectively is the most critical factor in becoming a successful systems analyst. The ability to converse (communicate) and deal with all types of people at every level in an organization is an attribute that a systems analyst must possess. While conducting a systems analysis study, it is not uncommon for an analyst to interview a member of top management and a DPSN (Data Processing Technician Seaman) keypunch operator in the same day. Very often, conflicts between the requirements of the user and the requirements of other branches of the ADP facility are identified during interviews. The systems analyst must be able to communicate the nature of these problems to all the branches and interface with them in each of the solutions. Most analysts are extremely versatile and resourceful when performing liaison duties between branches. When performing liaison and interfacing duties, the ability of the systems analyst to communicate knowledgeably is essential. The interfacing requirements of a systems analyst are summarized in figure 4-3.

SYSTEMS ANALYSIS

A systems analysis is not conducted exactly the same way in all situations. Once it has been



78.149

Figure 4-3.—Knowledge interfacing capabilities and requirements.

determined that a problem exists, the analyst must determine (1) what is taking place, (2) what should be taking place, and (3) what the user wants to take place. This could encompass an analysis ranging from a simple new report requirement to an analysis of a completely new system software/hardware requirement.

Since the Navy does not change computer systems very often, this chapter will relate to problems of software/hardware additions, changes, and modifications of input/output requirements of a command's parent computer system that has already been funded and systems approved.

Systems analysis involves collecting, organizing, and evaluating facts about an existing or proposed system and the environment in which it presently operates or will operate after it has been implemented. This requires determining the following user needs:

1. Inputs and outputs.
2. The data and information requirements of an organization for both operating and management purposes.
3. The sources of data.
4. The processing methods and files (Manual/Automatic) that serve as a link between input and output.

Systems analysis, as used in this chapter, is restricted to fact-finding and to examining present systems to determine problem areas. The reason for this restriction is because this type of analysis is applicable to existing systems.

The objective of a systems analysis study is to learn enough about the problem, system, equipment, personnel, and operating conditions, and the demands on these factors, to establish the foundation for designing or redesigning and implementing a better system, if it is found desirable or feasible to do so by upper management. A redesigned data processing system or information system is better only if it increases the overall output of the organization, considering the cost of systems design or redesign as part of the total cost.

Analysis Generation

Consider the question "What generates a systems analysis study?" The answer to this can vary as much as the ways in which an analysis can be performed. Usually, it will be for one of the following reasons:

1. The user has a problem in one of the software systems.
2. A new requirement of input or output data will change or create a new data base and report.
3. New users have additional systems requirements.
4. A new or changing requirement is initiated by management (internal or external).
5. The parent computer system cannot perform efficiently under present requirements.
6. A request for additional or new hardware requirements is generated.
7. Excessive material and resources are expended for a project which exceeds management's budget goals.
8. The present software or hardware system takes too long to produce the output the user wants.

9. There are frequent hardware or software failures.

10. There are frequent errors in command written programs.

11. There is dissatisfaction with the operating results of the ADP facility's present computer system. This would include insufficient or inaccurate information, excessive burdens on operating personnel to collect data, excessive system operating costs, or administrative ADP problems.

Facetiously speaking, the only time some type of analysis is not being performed is when (1) the system is operating perfectly, (2) no changes or new requirements exist, and (3) technological change in ADP hardware and software is at a standstill. Of course this status is never true, and some analysis is always being performed by the analysis branch. A system has not been developed that is perfect and cannot be improved. If you agree with the latter statement, you should consider applying for a DP-2751 systems analyst NEC.

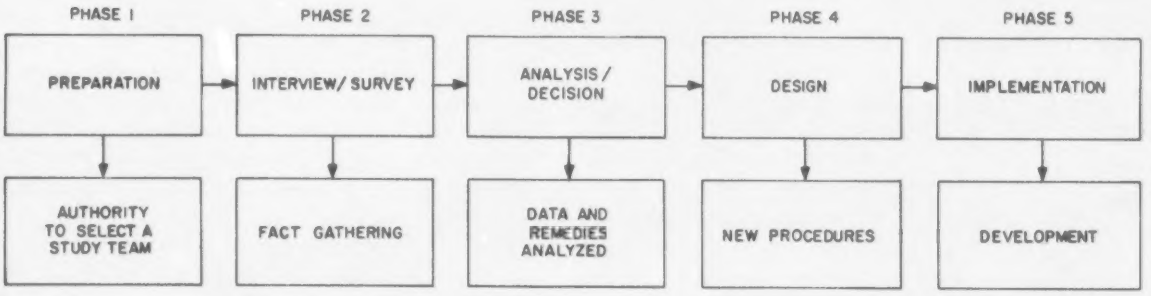
PHASES OF A SYSTEMS ANALYSIS STUDY

There are five phases in a systems analysis study for analyzing an existing funded system (fig. 4-4). For the purpose of this chapter, an analysis of an installed computer system will be emphasized. The five phases are mentioned briefly here and are discussed in detail later in this chapter.

1. Preparation Phase.–During this phase the analysis is approved by upper management and a systems analyst or a complete systems analysis study team is appointed to complete the analysis project, whichever is appropriate. Defining the scope of the analysis, setting schedules, and similar preparatory activities to lay the ground work for the full-scale study are included in this phase. As a general rule, the systems analysis study plan is prepared in this phase. This includes preparing appropriate questionnaires, collecting adequate blank forms, and becoming familiar with any special written guidance instructions or documentation from upper management.

2. Interview/Survey Phase.–In this phase all existing documentation concerning the analysis is reviewed; the present systems processing is surveyed (hardware/software); the data and files involved are determined; and the products, which are presently being obtained, are determined. This phase is accomplished by scrutinizing the documents used, conducting interviews, and collecting all facts pertaining to the analysis study.

3. Analysis/Decision Phase.–In this phase all the information, data, and facts pertaining to the analysis study gathered during the interview/survey phase is analyzed. A recommendation is submitted to upper management if the result of the analysis is



78.150

Figure 4-4.–Systems analysis study phases.

negative or not feasible for design and implementation.

4. Design Phase.—In this phase the systems analyst or systems analysis study team bring together the solutions for the problems of the present computer system or an approved new system if appropriate. The new software/hardware modifications are designated, processing and procedures are determined, and any other requirements are specified.

5. Implementation Phase.—In this phase additional equipment is selected and new systems programs are developed and tested. If additional hardware equipment is approved, it will be installed. Also, live tests are performed and evaluated. After the hardware and/or software modifications or additions have been accepted by upper management, the systems analysis study and team are dissolved until another modification is needed to the system.

THE ANALYSIS STUDY TEAM

When determining the total size of a systems analysis study team, upper management will appoint the team members in accordance with the workload involved in the analysis study. If a "total systems analysis" is undertaken, then the analysis study team should have enough analysts and non-analysts appointed to complete the project through each phase and be conducted in accordance with SECNAVINST 5231.1 (series latest revision). A total systems analysis may evaluate the entire ADP facility structure at every level when designing a new system. A total systems analysis approach (as detailed in SECNAVINST 5233.1 series) will not be emphasized in this chapter. An already funded project initiated at local ADP facility level will be discussed.

Each ADP facility has its own requirements and work-load responsibilities, and appoints the analysis study team members according to local requirements/needs. Usually not more than two analysts are assigned to analyze a small systems addition or modification. The reason two analysts are suggested is that an inexperienced DP-2751 systems analyst can be teamed with an experienced analyst qualified to complete the entire project.

When conducting a total systems analysis study, there are usually members appointed to the analysis study team that are not DP-2751 systems analysts. There is a great deal of work involved in an analysis study of this nature and expertise from all areas of the organization is required. Members are appointed to the analysis team from higher authority commands, upper management, middle management, operations, and programming, and include users, civilian and military engineers, and DP-2751 systems analysts.

PREPARATION (PHASE 1)

The first phase of a systems analysis study is the preparation phase. In many instances, this phase is skimmed over or rushed. This phase is very important, and the systems analyst in charge should devote adequate time, effort, and preparation to it. Following are the 10 basic steps in phase 1:

1. Approval for the analysis study is granted.
2. The team is appointed.
3. The scope of the analysis study is defined.
4. Time schedules for the analysis study are set.
5. The analysis study plan is prepared.
6. Questionnaires are prepared.
7. Blank forms for interviewing are prepared.
8. The analysis study team is indoctrinated.
9. Personnel interview schedules are coordinated.
10. The analysis study is begun.

When starting phase 1 of a systems analysis study, the team leader should give considerable thought to flexibility and not treat the 10 steps as an unchangeable procedure.

Approval (Step 1)

The first step of preparation (phase 1) is receiving approval to do the analysis study. This approval will usually be generated within the local command because it is already under

funded approval and concerns a problem that exists with the present system. When doing a total systems analysis, the approval will come from higher authority, down through the chain of command. A total systems analysis directed by higher authority usually indicates a large hardware or software change and is performed in accordance with SECNAVINST 5231.1 (series). For the purpose of illustration in this chapter, a hypothetical analysis is being performed on a problem using existing funded hardware and software. This type of analysis is approved by the parent ADP facility and is usually in the form of a project request approved by the commanding officer of the ADP facility.

Team Appointment (Step 2)

The second step of preparation (phase 1) is the actual assignment of the analyst(s) to do the analysis. The number of analysis study team members can range from one to as many as it takes to complete the analysis. This depends on how big the project is and the workload of the systems analysis branch. As stated earlier in this chapter, it is recommended that a minimum of two analysts be appointed to each project if inexperienced analysts are assigned to the analysis branch.

It is usually the responsibility of the officer-in-charge (OIC) of the systems analysis branch to assign members to the systems analysis study team for each project.

Scope (Step 3)

The third step of preparation (phase 1) is the defining of the scope of the analysis study. At this time the user, management section, or branch that requested the systems analysis study should have provided a clear and precise statement (with the project request) of what should be accomplished. This statement should identify the operation, the system or subsystem, or the areas that will be affected by the study. Generally speaking, the scope of the study is the problem described in detail by upper management and/or the user requesting the analysis study. Detailed information in the scope statement is very important because it sets the boundaries within which the analyst will work.

The scope of the analysis study should answer or identify the following list of problems (if they exist) for the systems analyst:

1. What are the nature and purpose of the work products desired?
2. Is this a new system or subsystem?
3. Is this a hardware or software problem, or both?
4. What data files are involved or will be created?
5. What new or old reports are involved?
6. Is existing documentation for the system or subsystem available and up-to-date?
7. What is the due date for implementation?
8. Are external resources or organizations involved?

If the scope of the analysis study is sufficiently described, it will permit the systems analysis study team to start visualizing the problem in a wider spectrum immediately. The scope statement is the document that gets the analysis off to a correct start.

Schedules (Step 4)

The fourth step of preparation (phase 1) is the setting of time schedules. After a thorough review of the scope statement, an experienced analyst should have a good idea of how long the analysis should take. This time factor should be discussed with all members of the systems analysis study team and coordinated with upper management. Always request enough time, and set milestones that are realistic.

Setting time schedules could be a major factor in the analysis if it involves an offsite total systems analysis study of an organization that presently does not have a computer system. If this situation exists, all travel time schedules should also be coordinated with the organization under study and the present upper management during this phase step.

Analysis Study Plan (Step 5)

The fifth step of preparation (phase 1) is preparing the actual analysis study plan. The

majority of the material needed in the analysis study plan should be collected and inserted into a bound document during the preparation (phase 1) (step 5). When drafting the analysis study plan, it should not be regarded as a final document, but as a starting tool, subject to change until the analysis study is completed. Later in this chapter an outline format for an analysis study plan is displayed in detail. The items and forms included will always vary, because every analysis study is different in some way. This outline is only a suggested procedure on how to prepare a problem for analysis. The following items, however, are common in every analysis study and should always be included in the analysis study plan:

1. The written authority to conduct the analysis study.
2. A written statement of the mission of the analysis study, the problem as it is known to exist, and what the survey is expected to accomplish.
3. A written statement assigning the analysis study team members, including each member's security clearance.
4. A schedule showing when each major step is to be accomplished and which team member will perform it.

Questionnaires (Step 6)

During the sixth step of preparation (phase 1) all locally designed questionnaires should be typewritten to completion except for information the questionnaire asks the recipient. Questionnaires should be locally designed to supplement personal interviews. The form should be designed for the computer systems hardware and software on which the analysis is being performed. The use of such questionnaires should be limited to situations where it is inconvenient to interview all of the individuals involved in the analysis in person. Following are some of the instances when a questionnaire can be useful as a fact-finding tool when personal interviews are prohibited:

1. In cases when the analyst and recipient are physically separated and travel is not feasible.
2. In cases when the recipients are too voluminous.
3. In cases when the information gathered is repetitious and will be used to verify similar data from other sources.

Interview Forms (Step 7)

During the seventh step of preparation (phase 1) the team leader should prepare interview forms and fill in data that is already available, such as:

1. Name of individual to be interviewed.
2. Project number.
3. Security of interview form (if known prior to the actual interview).
4. Department where individual is to be interviewed.
5. Phone number.
6. Status of individual; for example, DP1, GS-9, contracted civilian, etc.
7. Remarks section—list all appropriate questions pertaining to the analysis as can be determined for the problem under study for the individual being interviewed. Questions of this type help organize the material in logical sequence and keep the interview in order. The particular systems analysis study, project topic, and managements desired outcomes will derive the actual questions.

The analyst should be prepared to go to the interview with a documented list of questions pertinent to the analysis being performed. Without a thought-out list of prepared questions, the analyst may not generate all the required information, the interview could tend to ramble, and the analyst could appear "not too bright."

Study Team Indoctrination (Step 8)

During the eighth step of preparation (phase 1) the entire analysis study team should be oriented by the team leader. The team should be briefed on all aspects of the analysis and all pertinent information and material to be associated with the analysis, such as

organizational charts, functional charts, directives, regulations, instructions, policies, and documentation manuals relative to the analysis study. The briefing should also specify which forms are to be used and how they are to be completed, the people to be interviewed, and the required data to be collected.

Upon completion of the indoctrination briefing, the team members should have their work schedule and expected completion dates for each phase of the analysis.

Ample time should be given during the briefing to answer any team member's questions. It is essential that the team leader explain the assignments of and requirements of each team member in detail. Remember, the more detailed the indoctrination is, the better end-results will be accomplished in the analysis.

Interview Schedule Coordination (Step 9)

During the ninth step of preparation (phase 1) all interview schedules should be confirmed. The analysis team leader should arrange appointments as far in advance as possible and coordinate all interviews through department branch heads and division leading petty officers. When coordinating the interview schedules with these individuals, a thorough explanation of the analysis study should be given.

Analysis Study Commencement (Step 10)

During the tenth and final step of preparation (phase 1) all steps of preparation should be checked for completeness.

If time permits, it might be desirable to take an orientation trip to the branches involved in the analysis. In this visit, the analyst has the opportunity to meet concerned individuals and can break down any initial resistance to the forthcoming interviews.

INTERVIEW/SURVEY (PHASE 2)

The second phase of a systems analysis study consists of the interview and actual survey. There have been many different approaches taken toward this phase of a systems analysis study. These approaches have varied from a complete data gathering and fact-finding analysis to a cursory look at the problem that generated the systems analysis. These widely different approaches stem from the actual policies, needs, and requirements set forth at different commands.

When time and manpower permit, a complete and thorough analysis should be conducted using set procedures. The procedures for a small problem analysis should generally be the same as for a large project systems analysis. Every command should follow the documentation procedures set forth in the SECNAV 5233.1 series instruction, and other appropriate instructions for equipment acquisition (SECNAVINST 5230.6 (series)), operation, review, and evaluation.

The main purpose of the interview/survey phase is to gather facts. This is basically accomplished in the following three steps of phase 2:

1. Survey the problem using existing documentation.
2. Interview individuals in their environment.
3. Document and collect data.

Phase 2 of the systems analysis study should be started as soon as possible after the completion of phase 1 (step 10).

Problem Survey (Step 1)

The first step of the interview/survey (phase 2) is to ensure that the existing documented and operating procedures, as set forth in the documentation manuals, are currently up-to-date and are being adhered to in actual operations. If the problem being analyzed does exist and is not a new requirement, it is then necessary for the analyst to actually observe and survey current operating procedures of the project's software and hardware. It is extremely important that the analyst obtain copies of the actual forms, operating documents, and manuals that are currently being used in the

system and are pertinent to the problem under analysis.

The purposes of observation are many. It allows the analyst to determine the following facts:

1. What is being done.
2. How it is being done.
3. Who is doing it.
4. When it is being done.
5. How long it takes.
6. Where it is being done.
7. Why it is being done in its present manner.

This procedure is often very helpful to the analyst, because in many instances it is discovered that the systems documentation is incorrect and that actual procedures are different from what some of the interviewed people think.

Interviewing (Step 2)

The personal interview is the most powerful fact-finding tool available to the systems analyst. It provides the analyst with a means of getting information that may not be recorded anywhere except in the mind of the individual being interviewed.

An interview should be construed by an analyst as being a purposeful conversation, planned and controlled by the analyst, to gain a specific objective. An interview should be thought of as a face-to-face conversation rather than a professional interrogation. The interview that drifts into a confrontation of old-versus-new will produce nothing tangible for the systems analysis study. If the interview is conducted properly, it can produce meaningful, useful, and correct information.

In short, the interview is the tool used by the systems analyst to help resolve the project request that generated (originated) the systems analysis study. This is true whether the analysis is a simple project request for additional or modified reports, or a total systems analysis.

Conducting the Interview.–To start an interview in the right direction, the systems analyst should ensure that all interview appointments are kept on time in the interviewee's office, space, or environment. If at all possible, the analyst should not require persons being interviewed to leave their work areas. The interview should be conducted as informally as possible, yet consistent with the need for organized and planned results. Further, the systems analyst should be courteous without leaving the impression of being apologetic for interrupting the individual's work schedule with an interview.

As mentioned earlier in this chapter, the systems analyst should have a locally prepared interview form for each individual to be interviewed. A check list of questions may prove very helpful during the interview. Following is a list of some possible questions that might be used:

1. What items are maintained as file information?
2. What is the number of A/N (Alpha-numeric/Numeric) characters in each item in the file?
3. How many separate files make up the systems data base?
4. What are the source data?
5. What is done with the source data, step-by-step, during the performance of each operation?
6. What other data are used in each operational step?
7. What decisions are made in each operational step?
8. What normally recurring conditions are accounted for in each operation?
9. What exceptional conditions arise during the data processing?
10. Where are the exceptional conditions reintroduced into the operation?
11. What are the results (punched cards, documents, listings, reports, magnetic media, etc.) of each operation?
12. How frequently is the operation done?
13. What resources (personnel and equipment) are now utilized for the operation?
14. Are the source data processed in batches?
15. How many items are processed on an hourly, daily, or any other periodic basis?

16. How many items of output result from processing on the same periodic basis?
17. What deficiencies in processing are known to exist?
18. What deficiencies in source data are known to exist?
19. What deficiencies in output information are known to exist?
20. What are some recommendations for the new requirements?
21. What is your recommendation for the solution to the problem?

The preceding questions are just a few out of the thousands that could be asked during an interview. The ones created locally should be direct and pertinent to the problem under analysis.

During the interview the analyst should take notes. Notes help organize the material in logical sequence and clarify thinking. Facts are more reliable when they are immediately recorded. Individuals being interviewed might consider it insulting if a written record of their conversation is not kept; especially if they feel their answers cannot be remembered by the systems analyst. Further, this practice will help prevent the analyst from coming back after the interview to verify facts.

While it is important that a systems analyst have an excellent command of the English language, it is more important that this individual be a good listener. A good rule to remember is "you cannot obtain facts while talking." Observing this rule will give the interviewee the impression that the analyst is interested in what is being said.

There are many personal and professional traits that an analyst should either possess or control to make any interview a success. The following are just a few of the "do's" and "don'ts" that a systems analyst should consider during an interview:

1. Be on time for the interview.
2. Explain the problem and purpose of the interview.
3. Be a good listener and refrain from talking about subjects that are not pertinent to the problem being analyzed.
4. Ask frank and forthright questions.
5. Be courteous but not apologetic about taking up the interviewee's time.
6. Do not make disparaging statements.
7. Do not give the impression that you know more about the problem under analysis than the individual being interviewed.
8. Conduct the interview as informally as possible, but consistent with respect of the status of the individual being interviewed.
9. Avoid using ADP terminology (computer jargon) with individuals who are not ADP oriented.
10. Obtain ideas, opinions, and facts about the problem under analysis.
11. Do not make derogatory remarks about other individuals or present procedures.

Interviewing Problems.–There are special problems connected with interviewing, both in the analyst's attitude and in the interviewee's attitude.

As an analyst, it is easy to fail to take into account a preconception concerning the results you would like to obtain. That is, instead of objectively attempting to get the facts on a particular situation, the natural impulse is to arrive at a tentative conclusion and then attempt to get the necessary facts to back up some premature theory, already half-formed. Nothing could be more detrimental to a successful systems interview. Likewise, when a new situation arises, there may be an unconscious attempt to associate it with some past experience. Even highly experienced analysts, who may have used certain methods successfully in the past, have a tendency to attempt to "straightjacket" the existing situation into this previous experience.

During an interview, the analyst should be aware of the attitude of the person being interviewed; for example:

1. Nervousness–Many individuals are nervous under the actual strain of any type of interview. The more experienced analyst will notice this at the beginning of the interview and will explain that the interview is not formal in an attempt to set the interviewee at ease.

2. Over-response–Through a desire to cooperate, some individuals, when interviewed, have a tendency to supply answers that they feel are most favorable to the analyst, rather than to state the facts as they exist. Questions should be carefully worded to avoid suggesting an answer.

3. Conjecture and inaccuracy–Some individuals being interviewed may give information without actually checking the facts. This is true when the interviewee feels that he/she should already know the answer without having to look it up. Questions should be precisely worded to require specific and factual answers. When an analyst wants an opinion, the question should be so stated and noted in the recording of such information.

4. Cautiousness–Directly opposite to the overzealous person is the cautious individual who answers questions only when positive the answer is correct. This type of individual may withhold valuable information if not absolutely sure of its accuracy in every detail.

5. Resentment–Individuals with hostile or resentful attitudes toward what is under analysis are perhaps the most difficult sources from which to get information. They may have any number of reasons for not cooperating with the analyst. Some of these reasons are that they may be averse to change, fearful of losing their job to a machine, or just too busy to be bothered. A considerable amount of tact and resourcefulness must be called upon to convince this type of individual of the need for cooperating in the systems analysis study. The fears brought about by this type of attitude can be allayed by a careful explanation of the purpose(s) of the analysis.

Tone of the Interview.–The tone of the interview is a reflection of the mental and physical attitudes of the interested parties. If they are relaxed, friendly, and informal, the interview will produce positive results. It is mostly up to the analyst to bring about this desirable situation. Interest cannot be successfully pretended, but must really exist. People are quick to recognize sincerity and usually react to it in a favorable manner.

Remember never to give adverse criticism of the way things are presently being done, and never verbally express an opinion about the problem that is under analysis.

Guiding the Interview.–The interview should be limited to information and fact gathering. While free discussion should be encouraged, be careful not to be drawn into conversational detours about hunting, fishing, or other hobbies. The analyst should recognize that this is a waste of time and quickly guide the conversation back to the analysis.

Further, the analyst should be very reserved about making conclusive statements during an interview. This is neither the time nor the place for the analyst to make conclusions because all the facts have not been studied or even gathered.

Ending the Interview.–Prolonged interviews are rarely desirable. If it is necessary to discuss the problem of the analysis for more than an hour at one setting, the analyst should split the interview into two sessions. Interviews are hard work for both the analyst and the interviewee. The maximum time for any single discussion should never be more than an hour. If the interview is scheduled for an entire day, the appropriate thing to do is break every hour for a minimum of 5 minutes. If, as the interview progresses, it becomes evident that all the material cannot be covered in the allotted time, the analyst should make another appointment that is mutually convenient. Any question that was important enough to have been included in the systems analysis study outline should not be eliminated simply because it is not covered within a particular time period.

When the analyst ends the interview, it should be explained to the interviewee that additional time may still be required for verification of the notes taken during the interview.

Follow-up of Interview.–As soon after the interview as possible, the analyst should make a complete flowchart of the information gathered during the interview. Further, a good summary should be made from the interview notes, and

drawings of charts should be completed. When the information has been compiled by the analyst, a copy should be returned to the individual who was interviewed for verification, corrections, and additions. It is always advisable to have the interviewee sign the copy and return it for use in future phases of the analysis.

Document and Data Collection

By the time the systems analysis study has progressed to this point, many of the source data and documentation manuals describing the source inputs and outputs have been identified. As soon as possible after the interview, the systems analyst should collect samples of all the source data pertinent to the analysis and any other documents found to exist during the interview not already identified and reviewed. Once all operating and programming functions are identified and all supporting documents and source data (inputs/outputs) collected it is imperative that this information be recorded in a meaningful manner for analysis study. These compiled documents and sample source data will provide insight into how the existing or proposed systems operate or will operate. But this insight will not materialize unless the analyst and other members of the analysis study team have some designed means and techniques that will aid in the analysis of the documents and source data collected. In a system analysis of a small problem, only a few documents and a small amount of source data would be collected; in more complex systems analysis studies, the number of documents and source data collected could run into the thousands. When collecting any volume of documents and source data, it is necessary and practical to employ a worksheet for recording the information about a document or source data as it becomes available to the systems analyst. For example purposes in this chapter, this type of worksheet will be referred to as a Systems Analyst Document/Data Collection Worksheet (SAD/DCW). It is recommended that a similar form be designed as local conditions warrant and used while interviewing individuals and during actual document and source data collection. As shown in figure 4-5, an SAD/DCW is a self-explanatory form that can be reused to condense large amounts of reference data onto a single sheet of paper for each piece of data or document collected. This type of locally prepared form should contain actual facts and not opinions, since it is used later in phase 3 of the systems analysis study.

Other systems analysis tools that can be used in data and document fact gathering include flowcharts, grid charts, matrix charts and decision tables. Basically, it is up to the analyst to determine which tools to use and how thoroughly the systems analysis is to be conducted. Remember, the more facts that are gathered during this phase of the systems analysis the better will be the solutions during the analysis and decision phase.

ANALYSIS/DECISION (PHASE 3)

The third phase of a systems analysis study is the analysis of the documents and data collected, plus informational data generated by the analyst team thus far in the systems analysis study. This task sounds relatively simple, but in actuality, it can become very complicated, even for small projects such as an addition to an operating systems software already in existence.

After the interview/survey phase, the systems analysis team is likely to have quantities of detailed information gathered on the problem that generated the systems analysis study; the bigger the problem that generated the study, the more bits and pieces of information that will probably be collected for phase 3. The primary purpose of the analysis/decision phase is to analyze the bits and pieces, draw conclusions, and make recommendations to upper management concerning the assessment of the problem.

In previous phases, the analysts have collected documents and data on (1) what is being done, (2) who is doing it, (3) where it is being done, (4) when it is being done, (5) how it is being done, and (6) why it is being done in a particular manner.

The analysis/decision (phase 3) is often divided into four steps to provide a successful

SYSTEMS ANALYST DOCUMENT/DATA COLLECTION WORKSHEET (SAD/DCW)					
TYPE DATA/ DOCUMENT	DOCUMENT IDENTIFICATION		ORIGINATOR		INPUT SYSTEM
SOURCE DATA / DOCUMENT	FORMAT	VOLUME	LOCATION OF DATA		
INPUT / INTERMEDIATE DATA	SOURCE DESTINATION				
FINAL DATA OUTPUT	USE OF THIS DATA/ DOCUMENT				
DISPOSITION	FORWARDED	SUSPENDED	FILED	DESTROYED	CLASSIFICATION
HOW DATA PREPARED	RETENTION TIME	MEDIA TYPE	NO. OF MEDIA		
DOCUMENTS ORIGINATING FROM THIS AND BEING UPDATED BY THIS DOCUMENT/ DATA					
INPUT/OUTPUT RECORD FORMAT LAYOUT INCLUDING FIELD SIZE AND TYPE (A/N)					
(REMARKS ON REVERSE)					
DATE	ANALYST SIGNATURE		VERIFYING SIGNATURE		

78.151

Figure 4-5.—Systems analyst document/data collection worksheet (SAD/DCW).

and meaningful recommendation to upper management. The four steps are:

1. Document and data collating.
2. Analysis of facts.
3. Conclusions.
4. Recommendations.

Before the documents and data collected are reviewed, they should be arranged into some type of sequence. This is usually a time-consuming task, but the results of this organizing activity will make the copious mounds of information collected less cumbersome.

Document and Data Collating (Step 1)

The first step of the analysis/decision phase (phase 3) is to separate and sequence the documents and data previously collected in some orderly fashion. It should be apparent by now that each analysis study varies at least slightly from every other analysis study. Since this is the case, it is necessary that this step be performed according to the requirements of the problem under analysis. In most cases, the collected documents and data can be sequenced into four categories. The four categories are, document and data (1) inputs, (2) communications, (3) processing and storage, and (4) informational outputs.

The input to any system is that point at which data first enters the system or where a record is made of any action. Communications is the transforming of data from the point of entry to and between processing and storage points. Processing and storage is the method of receiving incoming data, transforming it into a medium which can be readily used by human or machine, and retaining it for retrieval by the user. The informational output of the system occurs when information is delivered from storage in a format suitable for the user to understand.

Analysis of Facts (Step 2)

By the time the analysis study team have reached this step of the systems analysis study, they should have a general, overall understanding of the problem under analysis. However, this is usually not enough to allow firm conclusions and recommendations of the systems analysis to be made. During this step of the systems analysis study, each document and each piece of data information should be studied in a meticulous manner.

It is recommended that the systems analysis team analyze the documents and data collected using the step-by-step procedure outlined in phase 3 (step 1).

Input.–To ensure that all of the information needed is obtained, it is a good practice for the analysis team to first study the facts about the input to the system. Some of the questions to be answered are:

1. What are the inputs into the system?
2. Where do the inputs come into the system?
3. In what form are the inputs?
4. What are the volumes of the inputs?
5. What are the frequencies of the inputs?
6. What and how many alphabetic and numeric characters are in each item of the source data?
7. What areas in the system do the inputs affect?
8. What is the reliability of the source?
9. What is the quality of the control for the source data?
10. Are all of the personnel processing the source data qualified and professionally knowledgeable?

It should be noted here that use of the preceding questions varies depending on the problem under analysis and the types of documents and data collected for the analysis. It would be impractical to attempt to list all of the types of questions pertinent to all of the types of analysis in a rate training manual.

Communications.–The record type of documents and data to be analyzed includes facts (source material) collected about

communications. Some of the questions to be answered may be:

1. What communication equipment is being used?
2. Are any special communications required, such as remote input, output, and inquiry?
3. What problems exist in these areas?
4. How many persons are involved?
5. Are present communications adequate?

An understanding of system communications enables the analysis team to determine how items of information and data are transmitted into and out of the system under study. This is the area where data transmission bottlenecks are often found. The analysts can then determine whether the communications are adequate or are being routed through areas that perform no action and are therefore superfluous.

Processing and Storage.–The third type of documents and data to be analyzed covers facts (source material) collected about the actual processing storage of data for a system. In most cases the source material collected in the area of processing and storage offers the systems analyst the greatest opportunity to analyze facts on how to improve the system, or how to solve the problem under analysis. The analysis of the material pertaining to processing and storage usually results in locating areas where duplication of effort, duplication of data elements, duplication of reports, and improper procedures are found.

Processing and storage, although closely related, are two separate areas. When analyzing material in the processing area, the analysis team should try to answer the following (or similar) questions:

1. How much of the operating system is required for processing each task?
2. What human decisions are made during processing?
3. What outputs are required?
4. How frequently is processing required?
5. How much processing time is involved (human and machine)?
6. What are the peaks and valleys of processing volumes?
7. What online and offline equipment is utilized during processing?
8. What programming language is utilized for processing?
9. What systems utilities are utilized for processing?
10. What is the abort ratio for software?

When analyzing the material (documents and data) collected in the storage area, the analysis team should try to answer the following (or similar) questions:

1. What files are maintained?
2. What types of files are maintained?
3. How many records are in the file?
4. How many items are in each record?
5. How often are the files updated?
6. What type of storage media is utilized?
7. What retention period is required?
8. Are data elements duplicated?
9. Can files be combined?
10. What access method is utilized?

Output.–The fourth type of material (documents and data) to be analyzed is made up of facts collected about the outputs of a system. The outputs of an existing system or the outputs of a requested system are the actual purpose of the system and are of prime concern to management. Whether the systems analysis team is analyzing collected facts pertinent to an existing system or a requested system, depending upon the scope of the systems analysis in accordance with SECNAVINST 5231.1 (series latest revision), the requirements of management are satisfied with actual output. It is the responsibility of the systems analysis study team to produce a timely and efficient means for the production of such system output. Some of the following questions should help the systems analysis study team to determine output requirements:

1. What are the outputs?
2. How are they prepared?
3. Can the present system produce the additional requested output (if any is required)?

4. How many copies are required?
5. What modification to the present system is required to produce any new reports?
6. Is the requested report produced in part as a whole by another system or subsystem?

After analyzing the different categories of material that were collected during the interview and survey phase, the analyst should have a thorough knowledge of the problem that generated the systems analysis. The analysis/decision phase of the systems analysis study should be executed to resolve all questions pertinent to the scope of the systems analysis. Naturally, the preceding sample questions are not pertinent in every type of analysis. The requirements set forth in the scope of an actual analysis will dictate what type of locally prepared questions should be asked about collected material. The locally prepared questions should produce information upon which to base conclusions about the material to be analyzed.

Conclusions (Step 3)

During the third step of the analysis/decision phase (phase 3) the system analysis study team should be prepared to agree on conclusions about the systems analysis study. Here again, it will depend on the scope of the analysis as to what type of conclusions will result.

Generally speaking, the analysis team should make their conclusions based on the FACTS gathered during the systems analysis. The following are just a few sample questions that can aid the systems analyst in making conclusions:

1. Has all the material pertinent to the scope of the systems analysis study been analyzed?
2. Is the project request feasible?
3. Can the project request that generated the systems analysis study be accomplished within the command or does it fall within the purview of SECNAVINST 5231.1 series and require higher authority processing.
4. Can the software/hardware be modified to accomplish the results requested?
5. Has each member of the systems analysis team reached the same conclusions?
6. Is the cost factor within command budget limits in accordance with SECNAVINST 5231.1 series.

When there is more than one individual performing the systems analysis study, there will always be the possibility that different conclusions could be drawn about a particular part of the analysis. If this happens, the member in charge of the systems analysis team should mention the differences when making recommendations to the official who authorized the study.

Recommendations (Step 4)

The fourth step of the analysis/decision phase (phase 3) is for the systems analysis team to make a written report to the official who authorized the systems analysis study. This report should be prepared intelligently and carefully with respect to all requested objectives within the original scope of the systems analysis study.

This report will contain different types of information, depending on the following two factors:

1. Whether the analysis study was authorized at a local level for an in-house problem involving software, hardware, or operating procedures.
2. Whether the analysis study was authorized by higher command authority directing a total systems analysis.

As stated earlier, examples of total systems analysis studies in accordance with SECNAVINST 5231.1 series are not thoroughly covered in this chapter. The following items should be contained in the report and forwarded to upper management for their review and approval:

1. Concise statements of anticipated benefits as a result of enacting the project request.

2. Specific recommendations, where deemed appropriate, for redesigning hardware configurations or software systems.
3. Precise statements with supporting reasons when recommendations are submitted to disapprove a project request.
4. A brief description of each modification, addition, or deletion required to the present software/hardware system.
5. Explicit statements for alternate avenues that could produce identical results in relation to the scope of the study.
6. Explicit statements of any additional requirement that was not included in the project request.

Sufficient detail should be included in the report to assist upper management in making a decision as to whether or not to authorize the design, documentation, development, and implementation of the project request.

If the project request is disapproved for implementation, upper management should take the following actions:

1. Notify the user of disapproval.
2. Send a copy of the systems analysis study team's recommendation report to the user.
3. Disestablish the analysis study team and reassign them to their normal duties.

DESIGN (PHASE 4)

In the fourth phase of a systems analysis study, the systems analyst utilizes past experience, ingenuity, and knowledge of all areas of data processing to solve the problem that generated the systems analysis study. The procedures and approach of the design phase of an analysis will vary, depending on the actual scope of the project request under study. For example, the procedures and approach for designing an additional software subsystem for an existing system would differ from that for a total systems analysis. A total systems analysis would involve designing a new hardware configuration, data bases, operating software, and preparing a Mission Element Need Statement (MENS) in accordance with SECNAVINST 5231.1 series. The likelihood of a Navy data processing technician designing a total system on any duty assignment is very unlikely. For the purpose of this rate training manual, a project request for an additional software subsystem on an existing funded system will be analyzed.

At this point, upper management has approved the project request and any modifications that were submitted at the end of phase 3. It should be mentioned here that some commands do not thoroughly perform phase 1, phase 2, and phase 3 because of heavy work schedules. Although it is not recommended to start a systems analysis at phase 4, it can and has been done by skimming over the previous phases. If only a cursory attempt to complete phase 1, phase 2, and phase 3 occurs, sooner or later, redundancy and duplication will exist in the installation's software, data base, and operating procedures. A paramount consideration in maintaining an optimum system is to avoid duplication. It should be remembered that systems analysis/design and optimum system performance are the responsibility of the DP (2751) systems analyst.

During phase 4 of most analysis studies, a new system is designed or an existing system is redesigned using four steps. These steps, in order of commencement, are (1) output design, (2) input design, (3) data base design, and (4) processing specifications.

Output Design Specifications (Step 1)

Through phases 1, 2, and 3 of the systems analysis study, the systems analysis study team determines what is needed as output from the system to meet the needs of the user and upper management. The design or redesign of systems starts with the design or redesign of the systems outputs. It is virtually impossible to design the input and processing procedures if the desired outputs and output formats are not first determined.

During this step of the analysis, the systems analyst should use the documents collected in the analysis and maintain a close liaison with the user while designing the new output content and

format. Also the systems analyst should at this time consider new documentation requirements. Any time a new system is designed or an existing system is redesigned a requirement for a new documentation is generated. Guidance on documentation is in chapter 7 of this rate training manual. At most commands the systems analyst branch will be involved with and sometimes responsible for certain documentation manuals such as the Data Requirements Document (RD), the System/Subsystem Specification (SS), the Program Specification (PS), and the Data Base Specification (DS).

When designing output requirements, the systems analyst should keep the following objectives in mind:

1. Design the output in a fashion to reduce the volume of information to a minimum (especially printed output) while being consistent with achieving the needs of the user.
2. Design the output so that it is easy to understand.
3. Design the output to be consistent with command policy.
4. Design the output on appropriate form layout sheets for the system under analysis, e.g., IBM forms, Honeywell forms, UNIVAC forms.

After the output content and format have been designed or redesigned by the systems analyst and approved by the user, the output media should be considered. Output media consideration is a very important part of output design. The following are just a few factors to consider when selecting the type of output media:

1. Cost–for example, printer paper versus CRT-hard copy
2. Storage–for example, cards versus microfilm
3. Speed–for example, magnetic tape versus disk
4. Efficiency–for example, console typewriter versus printer
5. Shipping–for example, disk versus printer listing
6. Durability–for example, paper tape versus magnetic tape
7. Retention–for example, CRT display versus microfilm

The variations in different output media and media type should be taken into careful consideration by both the systems analyst and the user.

Input Design Specifications (Step 2)

After the output content and format have been designed and approved by the user, the systems analysis team can then proceed to design the new input requirements. During this step of phase 4 the analysis team is simply defining and designing the data that must be brought into the system to produce the requested output. The types of data that will probably be considered as input are:

1. Actual output from other systems within the total system.
2. New source data created from source documents.
3. Data entered within a program from the results of computer calculations.
4. Extracted data from existing data bases.
5. Data keyed into the system during processing time.

It is essential that a new software system have accurate input to produce the desired output. If the input is haphazardly designed by the systems analysis team, it can almost be assured that the user will be dissatisfied with the results of the final output. The following procedures are suggested when designing input data and input media:

1. Utilize edited data whenever possible.
2. Design the input so that it is easily understood.
3. Design the input so that it is easily collected.
4. Keep the volume of data to a minimum that is required to produce the desired output.
5. Do not duplicate the source data resources.

6. Design the input data within the processing limitations of the computer characteristics.
7. Design the input data to match the desired input media.

Good input design and output results can be judged only by the user. The final step in designing input should always be the acceptance of the design by the user.

Data Base Design and Specifications (Step 3)

When designing a data base, the quality of data is a critical factor. Many of the considerations given to a conventional data base are also given to a system that utilizes a Data Base Management System (DBMS). Chapter 5 of this rate training manual discusses data bases in conventional format and in systems using the DBMS. The design techniques should conform to the structure of the data base presently being used within the system.

When designing any type of data base, the first design consideration should be the validation of input data for any application. Another key factor that should be considered during the design of a data base is the design of adequate audit trail for processing the data.

The data base design will actually start with the design of (1) input records, (2) input files (master and intermediate), and (3) input procedures. How well the system functions and the quality of output depend on the quality and dependability of the data base. It should be emphasized at this point that reports which are produced from files and data bases that contain erroneous information breed mistrust of the ADP community as a whole.

Processing Rules and Specifications (Step 4)

During this step the systems analysis team will actually design the procedures, programs, and utilities necessary to produce what the user has requested. The systems analyst who performs this step of the analysis should be thoroughly familiar with the operating and programming language capabilities of the operating system. It would be a complete waste of time, money, and effort if designed programs and procedures were beyond the capabilities of the computer's software and hardware.

The following software and hardware considerations are potential guidelines for designing a complete subsystem to an operating system:

1. Design program documentation and systems flowcharts for editing and validating data for files within the data base.
2. Design program documentation and systems flowcharts to create master and intermediate files.
3. Design program and utility documentation and systems flowcharts to extract data from files.
4. Design program and utility documentation and systems flowcharts to update the data base and files.
5. Design program documentation and systems flowcharts that will logically manipulate data into intermediate and final outputs.
6. Design documentation and systems flowcharts for procedures and software requirements that match hardware capabilities.

All of the systems analyst tools that were prepared in phase 2 and phase 3 are employed during the actual design or redesign effort. The tools that were used for fact gathering and analysis can now serve to effectively document, flowchart, and design the proposed change, deletion, or addition to the system. These tools were items such as decision tables, interview forms, SAD/DCWs, grid charts, and other locally prepared material utilized to perform the analysis study.

The systems analysis team should prepare a complete design with all specifications, in the form of documentation and systems flowcharts, for all outputs, inputs, data bases and files, and processing procedures. These designs and specifications should be prepared in such a

manner as to facilitate the actual physical and technical design produced by the programming, data base, and operations branch in phase 5 of the systems analysis. It should be emphasized at this point that it is not a function of the systems branch to perform the actual technical functions of programming and detailed data flowcharting. These functions are the responsibility of the programming, operations, and data base branches of most ADP facilities.

At the conclusion of the design (phase 4, step 4), most of the responsibilities of the systems analysis branch for the systems analysis study are complete. The major responsibilities that remain with the systems branch are the coordination and liaison duties between the user and the other concerned branches involved with the actual production requested in the project request that originated the systems analysis study.

At this point in the analysis the systems analyst should deliver the entire systems analysis study plan to the ADP department head for disbursement to the other branches that will be involved with the actual technical development.

The systems branch should be responsible for any additional coordination between the user and other branches required during the implementation phase.

IMPLEMENTATION (PHASE 5)

A total systems analysis study in accordance with SECNAVINST 5231.1 series has not been emphasized in this chapter. Earlier in this chapter it was stated that a systems analysis for a problem on an existing funded system and a total systems analysis that requires higher authority approval basically followed the same phases and steps. These procedures in general are true up to the implementation phase. At this point, because of the vast difference of requirements that exists between the two types of analysis, the general procedures for a total systems analysis in accordance with SECNAVINST 5231.1 series are given in Appendix I.

In contrast to Appendix I, the following is an analysis for a problem on an existing funded system. This type of local command generated problem analysis is usually completed in four steps. It is discussed throughout the remainder of this chapter.

Research (Step 1)

During the first step of the implementation phase (phase 5) of a systems analysis, the responsible branch, in this case the programming branch, should assign as many personnel as deemed necessary to complete the project request.

Once the programmer has been assigned, a thorough research and desk study should be made of the entire systems analysis study plan. After it has been determined that the work can be accomplished according to the specifications in the analysis study plan, the programmer in charge should coordinate completion time schedules, through the systems analyst, with the user.

Development (Step 2)

During step 2 of the implementation phase (phase 5), the programming, operations, or data base branch, (in most cases all three branches will be involved) will perform the technical requirements to develop the output the user requested in the project request. The user usually does not care about the machines, languages, procedures, and documentation that is required to complete this step; instead, the major concern of the user is simply the output. The systems output, therefore, should be developed to meet the user's requirements. This is accomplished by highly trained DP programmers, operators, and data base administrators who will make decisions on what procedures, documentation, languages, and operations will be required to produce the output.

SECNAV Instruction 5233.1 series, FIPS publications, and local command policy should

be followed for the technical development of any system.

Testing (Step 3)

During step 3 of the implementation phase (phase 5) all testing should be accomplished. The testing of all software should be implemented with test data input. After the successful completion of testing test data, actual live data (real source data) should be used as input. This should produce the results of the requested output.

During the testing stages, all operating, programming, and documentation requirements should be completed. Once these required procedures have been completed, the appropriate branch (the programming branch in this case) can coordinate through the systems branch for a final appointment with the user.

User Approval (Step 4)

During the fourth step of the implementation phase (phase 5) all concerned branches should meet with the user who submitted the project request. Once the user has reviewed and accepted the output, the systems analyst should submit the project request to upper management (the ADP department head) for production approval. Upon upper management's approval, the system can be put into production and the systems analysis study is complete until other modifications to the system is needed.

ANALYSIS STUDY PLAN OUTLINE

Once any analysis study has been completed, all analysts can look back and see where improvements and different procedures could have been used in the study. The following summation of the preceding procedures is given, not as a policy or standard, but to aid the DP2 and above in conducting a systems analysis study for a problem on an existing funded system.

AN ANALYSIS STUDY PLAN OUTLINE

PREPARATION (PHASE 1)

Step 1: Approval

Step 2: The team is appointed

Step 3: The scope of the study is defined

Step 4: Schedules are set

Step 5: The analysis study plan is prepared

Step 6: Questionnaires are prepared

Step 7: Blank forms (tools) are collected

Step 8: The analysis study team is indoctrinated

Step 9: Interview schedules are coordinated

Step 10: The analysis study is officially commenced

INTERVIEW/SURVEY (PHASE 2)

Step 1: Survey problem (project request) using existing documentation

Step 2: Interview all concerned individuals

Step 3: Document and data collection (source material)

ANALYSIS/DECISION (PHASE 3)

Step 1: Sequence collected documents and data

Step 2: Analyze facts about material gathered

Step 3: Make conclusions on what is requested in relation to what actually exists

Step 4: Make recommendations to upper management

DESIGN (PHASE 4)

Step 1: Complete output design specifications

Step 2: Complete input design specifications

Step 3: Complete data base design specifications

Step 4: Complete processing procedures and specifications

IMPLEMENTATION (PHASE 5)

Step 1: Submit analysis study for technical research

Step 2: Complete technical development

Step 3: Complete technical testing

Step 4: Receive user and management's approval for production implementation

CHAPTER 5

DATA BASE ORGANIZATION

This chapter provides basic information about data base organization and data base management techniques to aid the DP who is performing the duties of a Data Base Administrator (DBA). Authoritative references are cited throughout this chapter and are to be utilized when implementing any type of data organization, data base management system, or data element standards. This chapter should not be referenced as the authority to implement any data base organizational standards. It is intended only to assist the DP1 and DPC in data base management.

Numerous data management techniques have been designed and redesigned for computer systems purchased by the U.S. Navy, Army, and Air Force. With each new technique the manufacturer claims increased flexibility and speed. Consequently, because of the new terms and procedures inherent with each new technique, the DP is usually left in a state of confusion unless extensive and expensive schools are provided.

The increased awareness that data can be utilized as an effective organizational resource has led to a recognized need for disciplined control of all automated and nonautomated data. This control is embodied in a set of management procedures and technical functions which is characterized as "data base administration." At the present time, the term data base administration is applied to a conglomeration of duties and responsibilities for which the DP1 is held accountable, and for which few standards or guidelines exist. There is much interest in this emerging discipline, both in the Navy and in the civilian sector.

DEFINITIONS

The communication of facts and ideas depends upon a mutual understanding of terminology. This is particularly true in the rapidly growing field of information processing, in which there is a continuing need for a comprehensive source of technical terms and definitions.

For the purpose of clarifying and standardizing the terminology used in this chapter, the following terms, abbreviations, and definitions are provided:

1. Data: (a) A representation of facts, concepts, or instructions presented in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means; (b) Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

2. Data Base: (a) A set of data, part or the whole of another set of data, and consisting of at least one file, that is sufficient for a given purpose or for a given data processing system; (b) A collection of data fundamental to a system.

3. Data Base Administrator (DBA): A person or group of people responsible for managing, controlling, and organizing the data base for an organization. The responsibilities of the DBA include the control, definition, organization, documentation, protection, and efficiency of the data base.

4. Data Base Management Systems (DBMS): A Data Base Management System can be characterized as a generalized software tool

that provides a single, flexible facility for accommodating different data files and operations. A DBMS facilitates operations on data (definition, maintenance, storage, retrieval, output); it facilitates reference by name rather than by physical location; and it provides an environment that is not tied to a particular set of application programs or files.

5. Data Catalog: A software tool used to list all of the data elements in a data base.

6. Data Description Language (DDL): A language independent of a host language, such as COBOL, that is used to describe a data base. This language should have the ability to specify the physical description of the data; specify the logical organization of the data; and modify the stored physical and logical data description without necessarily affecting the programs processing the original data.

7. Data Element Dictionary (DED): A software tool used to describe each data element; i.e., to tell "what" it is.

8. Data Element Dictionary/Directory (DED/D): A software tool used to list, describe, and locate each data element in a data base. It provides a centralized repository of information about each data element in order to facilitate the management and control of, and access to the data base.

9. Data Element Directory: A software tool used to locate each data element; i.e., to tell "where" it is.

10. Data hierarchy: A data structure consisting of sets and subsets such that every subset of a set is of lower rank than the data of the set.

11. Data library: A collection of related files; e.g., in stock control, a collection of inventory control files.

12. Data logging: The recording of data about events that occur in time sequence.

13. Data management: (a) The function of controlling the acquisition, analysis, storage, retrieval, and distribution of data; (b) In an operating system, the computer programs that provide access to data, perform or monitor the storage of data, and control input/output devices.

14. Data medium: (a) The material in or on which a specific variable may represent data; (b) The physical quantity which may be varied to represent data.

15. Data name: A character or group of characters used to identify an item of data.

16. Dependent DED/D: A primary DED/D that is designed and implemented to be DBMS specific. It uses features of the DBMS to which it is tailored, while providing the DBMS with control and management of the data elements.

17. Direct access: The ability to obtain data from a storage device or to enter data into a storage device in such a way that the process depends only on the location of that data and not on a reference to data previously accessed.

18. Direct access storage device: A storage device in which the access time is, in effect, independent of the location of the data.

19. Direct address: An address that designates the storage location of an item of data to be treated as an operand.

20. Directory: A table of identifiers for and references to the corresponding items of data.

21. File: A collection of related records treated as a unit.

22. File layout: The arrangement and structure of data or words in a file, including the order and size of the components of the file.

23. Format: The arrangement or layout of data.

24. Freestanding DED/D: A self-contained DED/D that performs the basic functions of controlling and managing the data elements without dependence on a DBMS.

25. Indirect address: An address that designates the storage location of an item of data to be treated as the address of an operand, but not necessarily as its direct address.

26. Index: A list of the contents of a file or of a document, together with keys or references for locating the contents.

27. Input data: Data being received or to be received into a device or into a computer program.

28. Inverted file: (1) A file whose sequence has been reversed; (2) in information retrieval, a

method of organizing a cross-index file in which a keyword identifies a record; the items, numbers, or documents pertinent to that keyword are indicated.

29. Job Control Language (JCL): In a job, problem oriented language designed to express statements that are used to identify the job or describe its requirements to an operating system.

30. Library: A collection of related files. For example, one line of an invoice may form an item, a complete invoice may form a file, the collection of inventory control files may form a library, and the libraries used by an organization are known as its data bank.

31. List: An ordered set of items of data.

32. Primary DED/D: A separate and distinct software package that functions principally as a tool for identifying, locating, controlling, reporting, and manipulating the information about data elements in a data base.

33. Pushdown List: A list that is constructed and maintained so that the next item to be retrieved is the most recently stored item in the list; i.e., last-in-first-out (LIFO).

34. Pushup List: A list that is constructed and maintained so that the next item to be retrieved is the earliest stored item still in the list; i.e., first-in-first-out (FIFO).

35. Queued access method: Any access method that synchronizes the transfer of data between the computer program using the access method and input/output devices, thereby minimizing delays for input/output operations.

36. Random access: In COBOL, an access mode in which specific logical records are obtained from or placed into a mass storage file in a nonsequential manner.

37. Record: A collection of related data or words treated as a unit; e.g., in stock control, each invoice could constitute one record.

38. Secondary DED/D: A software package in which the data dictionary function exists, but is not the main purpose of the software. A secondary DED/D is usually embedded in another system, and serves as the file and predefinition mechanism for that system.

39. Software tool: A computer program, the rules, and the associated documentation that assists a data processing technologist in designing, developing, maintaining, and managing data and software.

Data is a very valuable and sophisticated resource to an organization, not unlike the more traditional economic resources. Data is used to influence upper managment decisions by providing timely and accurate information. Therefore, it is very important that data as a resource be easily accessible, and essential that it be properly and effectively managed.

Before getting into file and data base structures, standard data elements, data description languages, and data base management systems, a close look at the individual who creates, manages, and manipulates these data software tools should be observed.

DATA BASE ADMINISTRATION

Data base administration is a growing concern of management. Data base administration encompasses all the technical and management duties required for organizing, creating, maintaining, and directing the data base environment. Over the years, data resources in the Navy have grown in size and complexity. It is apparent that not all of the data problems within the Navy are resolved with the use of software tools. Although software tools such as the DBMS, DED, and DED/D are needed to handle the influx of larger and more efficient data bases, these software tools create more administrative duties and tasks for the DP.

Some ADP facilities have established data base branches (sections/divisions) within the organizational structure to create, coordinate, maintain, and direct data base uses. Within this structure, the DP performs the functions and duties of a Data Base Administrator (DBA).

The main goals of data base administration are:

1. To optimize usage of data in a shared data base environment.

2. To incorporate a systematic methodology for the centralized management and control of data resources.

3. To balance conflicting objectives with respect to the organization's mission and the overall economy of data handling.

Among the key requirements for effective data base administration are:

1. An ardent support and commitment by local command upper management.
2. A technically competent DP staff.
3. A team participation in the data base environment by the management, DP DBAs, systems analysts, programming staff, operations staff, and users.

There are significant advantages that can be derived from a well-formulated data base administration policy. Some of these advantages are:

1. The data base can be better managed, especially if the data resources are centralized and shared.
2. Data independence can be accomplished through controlled definition, design, and implementation of the data base.
3. Data redundancy and inconsistency can be reduced by balancing conflicting requirements.
4. Data integrity can be improved by implementing standard usages, increasing data reliability, and enforcing security restrictions.
5. Increased responsiveness to the various user communities can result from better controlled and more up-to-date data.
6. Economic benefits can be derived by eliminating unnecessary duplicative processing.

The degree to which data base administration should be applied depends on the size and complexity of the data bases. Mostly, the application of data base administration depends on the informational needs and procedures of the local command. However, proliferating data bases, overlapping requirements, lack of data integrity, and duplication of effort are indications of the need for data base administration.

DATA BASE ADMINISTRATOR FUNCTIONS

Most ADP facilities have found it advantageous to let DBA functions develop gradually since they often counter more traditional approaches to data processing management and organization. In recent years, with the development of more complicated and sophisticated software, such as the DBMS, it became apparent that a need exists for individuals with more technical expertise and knowledge in data management.

The DBA for an ADP facility should normally be a DP1 or above and be appointed with positional authority to control all aspects of the data base. The DBA should coordinate all unusual requests or violations of command policy concerning the data base with upper management. The six basic qualifications an individual should possess before being appointed as a command's DBA are:

1. Coordination Ability—A DBA should possess an excellent command of the English language and be able to converse as an amicable arbitrator between users and other staff members.

2. Organization Knowledge—A DBA should have a thorough knowledge of the command's mission for long-range data base planning.

3. DBMS and DED/D Knowledge—A DBA should possess a thorough knowledge of the software tools present on the system to which the DBA is assigned.

4. Operations Background—The DBA should possess a minimum of 3 months operations experience (or the educational equivalent) on the system to which assigned. A thorough knowledge of the operating software characteristics, hardware, and teleprocessing procedures is essential when making decisions about the systems environment.

5. Programming Background—The DBA should possess a minimum of 3 months programming experience (or the educational equivalent) on the system to which assigned. A thorough knowledge of the host language in which the DBMS functions is essential when making software recommendations about data manipulation.

6. Documentation Background—The DBA should have a thorough knowledge of the

following higher authority directives and instructions:

(a) SECNAVINST 5200.18 (series) (latest revision)
Subj: Data Elements and Data Codes Standardization Program

(b) SECNAVINST 5200.19 (series) (latest revision)
Subj: Data Elements and Data Codes Standardization Procedures

(c) SECNAVINST 5200.20 (series) (latest revision)
Subj: The Department of the Navy Catalog of Standard Data Elements and Related Features

(d) SECNAVINST 5210.11 (series) (latest revision)
Subj: The Department of the Navy Standard Subject Identification Codes

(e) SECNAVINST 5233.1 (series) (latest revision)
Subj: Department of the Navy Automated Data Systems Documentation Standards

The DBA, in theory, is the ADP facility's leader in planning, designing, developing, implementing, testing, documenting, operating, and maintaining the data base environment. The role of the DP DBA is usually characterized as both technical and administrative. The DP DBA represents the "data base administration concepts and procedures" to all participants, and coordinates all data base activities among management, analysts, programmers, operators, and users. It should be noted that although the tasks in data base administration are sometimes performed by more than one DP, there is usually only one individual at a command who is charged with the responsibility for coordinating, controlling, and directing activities in the data base environment. This DP is generally designated locally as the DBA because, at present, no NEC or authorized official billet exists.

Although there is agreement on the basic functions of data base administration, there is no standard set of duties and responsibilities for a DP DBA.

The subject area of the tasks most commonly performed by DP DBAs is compiled in the following paragraphs. It should be reemphasized at this point that this rate training manual is not to be referenced to implement any function for a command, but is provided only to assist the DP in training.

DATA BASE DEFINITION FUNCTION.–The DBA should identify and define common data elements and define the relationships between data elements and other components such as programs, files, and systems. (Some definitions must be derived through negotiations with various users). The definition of the data elements and the data relationships should be based on a clear understanding of each participating user community's requirements, as well as the command's overall needs. Where possible, the DBA should use a data definition language to define and structure the data base (the CODASYL Data Description Language (DDL) will be referred to later in this chapter). It should also be in the DBA's purview to define, review, and monitor data standards in accordance with higher authority instructions. If the need arises for changing and restructuring the data base, the DBA should coordinate with upper management, initiate appropriate internal activities, and redefine the data base to meet the changing requirements.

TOOL SELECTION FUNCTION.–The DBA should participate in the evaluation, selection, and procurement of new hardware, software, and services related to data base administration.

DATA BASE DESIGN FUNCTION.–The DBA should take into consideration the differing needs of the entire user community during data base design. A data base should be designed to serve all users and represent all of their interests. Complex data structures are required to support the various facets of multiple users. This function includes:

1. The design of the data structure, as seen by the programming community.
2. The storage structure of the data base.

3. The mapping and search strategies.

4. The access methods utilized for the data base.

5. The design of the DED/D and of support software for creating, maintaining, and reorganizing the data base.

DATA BASE CREATION FUNCTION.–Under the data base creation function are included activities such as data collection; data base loading and testing; and implementation of data definitions, the DED/D, and other data base support software.

DATA BASE SECURITY FUNCTION.–The data base security function is intended to guard against unauthorized access to the data base, unauthorized update, copying, removal or destruction of any part of the data base. Data base integrity is related to the DBA's responsibility for the correctness and accuracy of the data. It can be achieved through the use of validation checks, loggings, dumps, backup and recovery procedures, and auditing procedures.

DATA BASE MAINTENANCE FUNCTION.–The DBA should be responsible for the continued well-being of the data base environment. As such, it should be the DBA's responsibility to maintain and update data base definitions and data base documentation. Further, it should be the responsibility of the DBA to maintain and update the DED/D and other data base support software. The DBA should follow and administer upper management's policies related to the data base, and define rules of use and access constraints for the data base. In addition, the DBA should be responsible for review and approval of new data definitions and enforcement of data standards in accordance with higher authority instructions.

COORDINATION FUNCTION.–The DBA should have a good rapport with users, programmers, operators, and upper management to facilitate the completion of daily tasks in a successful manner. The DBA should give assistance and guidance on the use of data base facilities and notify all concerned individuals of changes in the system's status.

DBMS VS DMS

Before going any further in this chapter, it is necessary to clarify what is meant by Data Base Management Systems as opposed to a similarly named but distinctly different class of software called Data Management Systems. The use of these two terms within the ADP community has been used rather loosely and has led to massive confusion on the part of the uninitiated.

A Data Base Management System can be defined as a software system that is intended to manage and maintain data in a nonredundant structure for the purpose of being processed by multiple applications. A Data Base Management System organizes data elements in some predefined structure, and retains relationships between different data elements within the data base.

A Data Management System, on the other hand, is one that is intended primarily to permit access to and retrieval from already existing files (usually for a single application). Although a Data Management System may be capable of minimizing data redundancy and centralizing the storage of data, the principal intent of the system is to perform such functions as information retrieval, report generation, and inquiry for a single application.

MANAGEMENT TOOLS FOR DATA ELEMENTS (DED/D)

The explosive growth of data bases, both in size and complexity, has made imperative the need for tools to aid in centrally controlling the data base definitions and accesses; for tools to manage the growth and changes occurring in a data base; and for tools to provide information to the different types of users within an organization. Data Base Management Systems (DBMS) have been designed and used to meet the information requirements for management of the organization.

A recent trend, however, is to use a separate class of automated tools for controlling/managing data elements in a uniform manner, across organizational lines. These

automated tools, Data Element Dictionary/Directory (DED/D) systems, while performing some of the same functions as the DBMS, are different in that their main thrust is in providing control over all the data resources, automated and nonautomated, within an organization. The functions of defining, describing and controlling the definitions and descriptions of the data elements are an integral part of the DED/D; that is, it is not just a cross-referencing or report generating tool.

Early designs of data processing systems revolved around specific application systems; likewise, the data was organized so that it would be machine and application specific. Thus, the data seldom crossed operational, functional, or organizational boundaries. This situation resulted in multiple definitions of the same data as independent data files were generated, thereby creating much redundancy and overlap.

As the role of the computer grew within the Navy, the need for system integration was evident, particularly with respect to data. The advent of Data Base Management Systems (DBMS) helped solve many of the information problems by organizing the data elements to which they were applied. DBMS can be characterized as generalized software which provides a single flexible facility for accommodating different data files and operations, while demanding less programming effort than conventional programming languages (DBMS will be discussed later in this chapter). Although the DBMS did not fully integrate all data resources within the Navy, they helped unify many of those resources.

Many of the benefits realized from the use of a DED/D are parallel to the ones attributed to the use of a DBMS. However, it should be noted that while the benefits realized from the DBMS are directly related to the effective computer processing of the data, the benefits from a DED/D are directly related to the effective collection, specification, and management of the total data resources of an organization. The tangible benefits that can be derived from the use of a DED/D and/or a DBMS are summarized in figure 5-1.

Benefits of a DBMS	Benefits of a DED/D
• The amount of redundancy in stored data can be reduced	• Simple and effective control of the data elements
• The problems of inconsistency in stored data can be avoided	• Reduction of data redundancy and inconsistency
• Stored data can be shared	• Enforcement of standard usage
• Standards can be enforced	• Enforcement of security safeguards and controlled accessibility to the data base
• Security restrictions can be applied	• Determination of the impact on the total information activity from changes to data elements
• Data integrity can be maintained	• Centralization of data elements as an aid in design and development of new systems
• Conflicting requirements can be balanced	• Consistency in documentation for data elements

Figure 5-1.–Organizational advantages through the use of information resource control.

Description of Automated Tools

Automated tools for the management of data elements provide a centralized repository of information about each data element in order to facilitate access to and control of the data base. These tools do not manage the actual content of the data, but they do manage the descriptive characteristics of that data; that is, its physical properties, such as length, value range, types of admissible characters, and validation criteria. They also control the usage of the data elements, such as what person or program is allowed to access and/or change the data elements. They further define the relationship of the data elements with each other, and with other components of the system. The use of automated software tools should reduce data redundancy, assure standard usage of data elements, and maintain data integrity.

These software tools are variously called catalogs, dictionaries, directories, and dictionary/directories. The deciding factors about what to call the package should be the amount and type of information that are provided the user. The nomenclature in figure 5-2 will prove helpful. Since most of the commercially available packages are of the Data Element Dictionary/Directory (DED/D) type, this group will be discussed.

Term	Definition
Data "catalog"	Simply lists all of the elements
Data Element "Dictionary"	Describes each data element, i.e., tells what it is
Data Element "Directory"	Locates each data element, i.e., tells where it is
Data Element "Dictionary/Directory"	Describes and locates as well as lists each element, i.e., tells both where and what it is

Figure 5-2.—Nomenclature of automated tools.

Data Element Dictionary/Directory

The Data Element Dictionary/Directory is a software tool that provides the means for defining and describing the characteristics of a data base, as opposed to the contents of a data base. Basic features of a typical DED/D are described below in the following paragraphs.

Typically, a DED/D has the following basic characteristics:

1. It contains a unique identification, a set of physical characteristics, and a textual description for each of the data elements.
2. It shows the relationships of elements to each other and to components of the system, for example, programs and reports.
3. It specifies the source, location, usage, and destination of the elements.
4. It has validation and redundancy checking capabilities.
5. It contains security safeguards for control of the accessibility to the data elements.
6. It has a command language.
7. It has reporting capabilities, such as:
   a. Predefined management-oriented, statistical analysis of summary reports
   b. Ad hoc, user defined reports
   c. Cross-reference reports
   d. Elements usage reports
   e. Audit trail reports
   f. Change effect reports
   g. Error reports
8. It has retrieval capabilities, such as keywording, indexing, and online batch querying.
9. It has facilities for interacting with a DBMS.

The commercially available packages have most of the preceding characteristics, as well as other features that distinguish each system from the rest.

The basic intent of DED/D's security features is to control the access to the data elements. However, this feature can also be used to protect the integrity of the data base, as well as to enforce predetermined conventions. Security features are present in all DED/Ds, although their extent and implementation vary in DED/D systems that make use of host system or operating system security provisions. Depending on local command policy, there is multilevel access control; the data administrator has the highest level of control–that is, has the ultimate authority for creating, updating, deleting, and accessing all data elements–and different levels of security are assigned to analysts, programmers, and various classes of users of the data elements.

DED/Ds can be grouped according to whether their dictionary/directory function is the primary one, or is secondary. Further, primary DED/Ds can be subdivided into freestanding and/or dependent categories, according to their implementation. Figure 5-3 presents a schematic representation of this classification.

Primary DED/D

A primary DED/D is a separate and distinct software package that functions mainly as a tool for identifying, locating, controlling, reporting, and manipulating the information about data elements in a data base. It is a basic tool within the data base environment that can assist the data administrator, the systems analyst, and the programmer in managing, planning, and evaluating the collection, storage, and usage of the data resources.

DED/D Function	DED/D Implementation
Primary	Free-Standing or Dependent
Secondary	Dependent (By definition)

Figure 5-3.–Classification of DED/D's by function.

The existence of primary DED/Ds as separate entities, rather than as a part of another system, is a recent innovation in the area of data management. They may be implemented in such a way that they may require a DBMS to function properly. A further subdivision of the primary DED/Ds clarifies the implementation of these packages: freestanding or dependent. It should be emphasized that both subcategories function principally as data dictionary/directory systems, and that they are different only in their implementation.

Freestanding DED/Ds are self-contained, and perform the basic functions of controlling and managing the data elements. However, they may use programs not specifically written for the DED/D, in order to enhance their capabilities and performance.

A freestanding DED/D may support one or more DBMS through the use of interfaces, achieving mutual benefit from this association. It should be emphasized that the freestanding DED/D does not depend on the DBMS to function; however, the use of DBMS interfaces can provide the data base administrator with a greater degree of control over the DBMS. It is possible for freestanding DED/Ds to have interfaces to more than one DBMS, sometimes simultaneously. Freestanding DED/Ds are also known as "generalized DED/Ds" in the civilian market.

Dependent DED/Ds are separate software systems that are specifically tailored to a general purpose DBMS. They provide the DBMS with control and management of the data elements by supplying the DBMS with the description, definition, location, and cross-references of the constituent data elements. In turn, DBMS resources such as file structure and access methods are made available to the DED/D. Dependent DED/Ds must perform all the functions of freestanding DED/D's.

Because the dependent DED/D is designed and implemented to be DBMS specific, the portability of this type of DED/D is restricted to installations having that particular DBMS.

DED/D Relationship to DBMS

Because DED/Ds are concerned with the management of data elements, it is logical that

there should exist a strong relationship between a DED/D and a DBMS. In this chapter, DED/Ds are categorized as "freestanding", with the capability to interface with a DBMS; or as "dependent", needing a DBMS.

It should be noted that freestanding DED/D's can have interfaces to more than one manufacturer's DBMS. Moreover, these interfaces can be supported simultaneously, so that where more than one DBMS is operational, the DED/D having multiple interfaces can generate the data definitions for all of the DBMSs, without having to "disconnect" any of the interfaces. The implementation of interfaces varies considerably from system to system and from manufacturer to manufacturer. The variance may be due to the way that the control blocks are generated, or it may be in the way that the DED/D supports the DBMS.

Interfaces enhance the usefulness of both the DBMS and the DED/D by providing the user with the ability to:

1. Define the data base to the DED/D, capitalizing on DBMS resources such as existent, well-defined file structures and access methods;
2. Generate data element description for a DBMS from an up-to-date DED/D; and
3. Exercise control over the data elements of a DBMS using DED/D facilities.

Secondary DED/D

A secondary DED/D is a software package in which the data dictionary function exists, but is not the purpose of the software. Secondary DED/Ds usually are embedded functions within another system; they serve as the data and file predefinition mechanism, and are an integral part of another software system.

Among the major differences between a primary and a secondary DED/D are:

1. The primary DED/D is a self-contained system, whereas the secondary DED/D is an internal function of another software system.
2. The reporting and retrieval capabilities are extensive for the primary DED/D, and limited for the secondary.
3. Primary DED/D's have more extensive security control over the data elements.

Since secondary DED/D's are embedded within another software system they are necessarily oriented towards the characteristics and internal representation of that system. It is impossible to separate their functions from those of the software system they serve. The emphasis in this section of this chapter is on primary DED/Ds; secondary DED/Ds are included only to complete the classification in figure 5-3.

Summary on DED/D

Among the major advantages of utilizing a DED/D are:

1. A central, consistent source of information about data is provided to the organization.
2. Consistent and timely documentation about data resources is provided to upper management.
3. A tool for controlling and maintaining the data resources of an organization is provided to the data base administrator.
4. A tool for data base and application design is provided to the system analyst.

Some disadvantages of utilizing a DED/D are: it can be time-consuming to install; the maintenance function may require considerable effort; and there may be objection to the formality necessitated by the DED/D.

Another drawback is that such a system is usually tailored to a specific application, and may not be flexible and responsive to changing requirements.

Sometimes the choice of a commercial system may be influenced by the fact that a DBMS is already operational within the organization. If there exist DED/Ds tailored to that DBMS, the DBA and upper management can consider dependent or freestanding DED/Ds having interface capability with that DBMS. Choice may also be influenced by the degree of support given a package. Of course, cost,

availability, and specificity are critical factors in the purchase/lease of a DED/D system.

DATA BASE MANAGEMENT SYSTEMS

A DBMS is a software tool that provides an integrated source of data for multiple users, while presenting different views of that data to different users. It can be characterized as generalized software which provides a single flexible facility for accommodating different data files and operations, while demanding less programming effort than conventional programming languages. It features easy access to the data; it facilitates the storage and maintenance of large volumes of data; and, most importantly, it provides the capability for sharing the data resources among different types of users.

Data Base Management Systems range from elementary systems with single record structures, providing rudimentary report formatting facilities, to very elaborate systems handling several files with hierarchical structures, performing functions in an online mode, and having sophisticated query and report writing capabilities.

So far in this chapter it has been emphasized how great the DBMS concept is and what problems can be solved by its utilization. By concept, DBMS is fantastic, but not all of the problems have been solved within the software by any commercial manufacturer. Like any new idea, concept, or methodology, it has had growing pains. DBMS is being used on a wide variety of computers in the Navy today. Because of this, no one DBMS by any single manufacturer will be discussed in this chapter.

Most of the problems with DBMS in Navy computer systems are the same as in the commercial community. A few of these problem areas are in the following list.

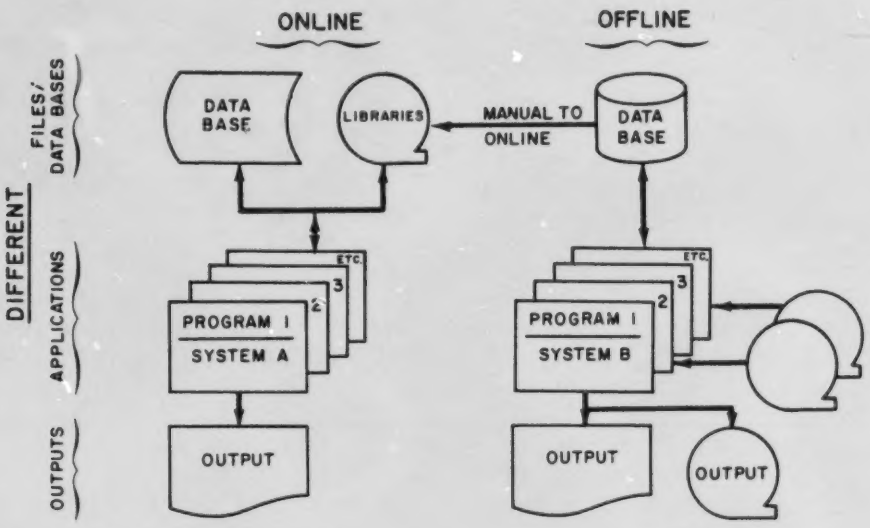
1. Users do not want to share their data with others in the data base.
2. There is no proper data representation.
3. Privacy and safeguarding of proprietary information are not sufficient.
4. There are different views of data by technical and nontechnical DBMS users.
5. There is no proper data structure for all applicable users.

The wide use of DBMS in the Navy indicates that all or most future operating systems will be oriented primarily toward DBMS. Slowly but surely, the DBMS problems in the preceding list are being eliminated through better and more sophisticated software, coupled with advanced training of users on such software usage.

Take a look at the changes that have been made from the conventional system file structure to the data base management system structure. As shown in figure 5-4, a conventional system is many application programs or systems using different data bases and files. These data bases and files are systems that are either online or offline; at any rate, they must be online at execution time. Under a conventional system, if data was needed in SYSTEM A and SYSTEM B, it was usually duplicated. This redundancy of data is not acceptable to the ADP community. The following problems are just a few of those that exist when redundancy of data is required.

1. Excess storage is required.
2. An excessive number of personnel are required to handle and manipulate the data.
3. A greater chance of error is possible when updating all the common data in different data bases and files.
4. An excessive amount of funds is expended for report production for management.
5. An excessive amount of CPU time is expended when collecting data for reporting.
6. A greater chance of error is possible in data integrity.

In many Navy ADP installations, a DBMS has produced a better record in operations and productivity than its predecessor, the file management system. DBMS has only a brief history to document its worth. DBMS software evolved from many different software improvements, from many different manufacturers; for example, from the IBM's IMS



78.152

Figure 5-4.—A conventional system.

software to the Cullinane Corp.'s IDMS software. None of the many DBMSs function exactly the same. Regardless of the manufacturer's software installed at a particular ADP installation, a basic DBMS can be conceptually depicted as shown in figure 5-5.

The next few sections discuss the events that take place when an application program of a particular software system needs (READS) a record. Before pictorially depicting a DBMS execution event, SCHEMAS, SUBSCHEMAS, a DDL, and a Data Manipulation Language (DML) need to be discussed.

Schema

A schema is a complete description of a data base, and consists of DDL entries. It includes the names and descriptions of ALL of the areas, set types, record types, and associated data items and data aggregates as they exist in the data base and are known to the Data Base Management System (DBMS). In other words, it is the overall logical data base description or framework into which values of data items can be fitted. A schema can be viewed like the bins in a storage house holding supplies. The schema will not change, but the data values will.

Schemas and subschemas differ from one software system to another and from one application to another. Because of limited space in this rate training manual, schemas and subschemas will not be depicted.

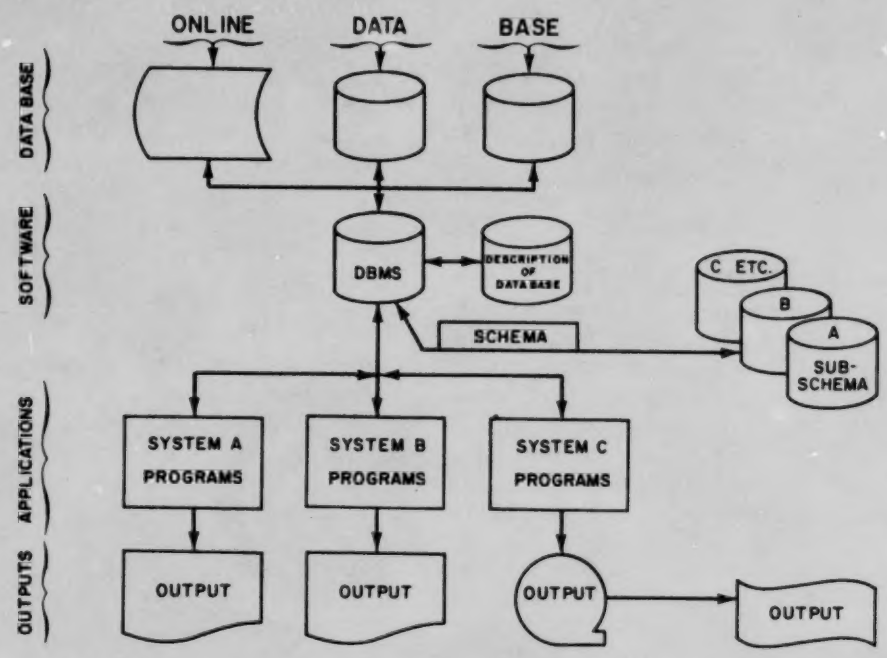
Subschemas

In addition to the schemas is the SUBSCHEMA.

The subschema is the applications programmer's view of the data within the data base pertinent to personal use or interest. Naturally, there are usually more than one programmer and one application on a software system, so there are usually many different SUBSCHEMAS for each SCHEMA.

The following are just a few of the many reasons subschemas are used.

1. The user and programmer do not need to know what data is contained in the entire data base.



78.153

Figure 5-5.–DBMS.

2. Subschemas enhance security factors and prohibit data compromise.

3. Subschemas aid the Data Base Administrator (DBA) when implementing data integrity.

NOTE: A subschema has access to those areas, set types, record types, data items, and data aggregates of interest in the pertinent application to which it was designed.

Schema DDL

The SCHEMA DDL is used for describing a DATA BASE, which may be shared by many programs written in many languages. This description is in terms of the names and characteristics of the DATA ITEMS, DATA AGGREGATES, RECORDS, AREAS, and SETS included in the data base, and the relationships that exist and must be maintained between occurrences of those elements in the data base.

A DATA ITEM is an occurrence of the smallest unit of named data. It is represented in a data base by a value.

A DATA AGGREGATE is an occurrence of a named collection of data items within a record. There are two kinds–vectors and repeating groups. A vector is a one-dimensional sequence of data items, all of which have identical characteristics. A repeating group is a collection of data that occurs a number of times within a record occurrence. The collection may consist of data items, vectors, and repeating groups.

A RECORD is an occurrence of a named collection of zero. one, or more data items or data aggregates. This collection is specified in the schema DDL by means of a record entry. Each record entry in the schema for a data base determines a type of record, of which there may be an arbitrary number of record occurrences (records) in the data base. For example, there would be one occurrence of a

PAYROLL-RECORD type of record for each employee. A DATA BASE KEY is a unique value which identifies a record in the data base to a run unit (program(s)). The value is made available to the run unit when a record is selected or stored and may be used by the run unit to reselect the same record.

A SET is an occurrence of a named collection of records. The collection is specified in the schema DDL by means of a set entry. Each set entry in the schema for a data base determines a type of set, of which there may be an arbitrary number of set occurrences (sets) in the data base. Each type of set specified in the schema may have one type of record declared as its owner type of record, and one or more types of records declared as its member type of record. Each set occurrence (set) must contain one occurrence of its defined owner type of record and may contain an arbitrary number of occurrences of each of its defined member type of record types. For example, if a set type QUALIFICATIONS was defined as having owner record type EMPLOYEE and member record types JOB and SKILL, each occurrence of set type QUALIFICATIONS must contain one occurrence of record type EMPLOYEE, and may contain an arbitrary number of occurrences of record types JOB and SKILL.

An AREA is a named collection of records which need not preserve owner/member relationships. An area may contain occurrences of one or more record types, and a record type may have occurrences in more than one area. A particular record is assigned to a single area and may not migrate between areas.

A DATA BASE consists of all the records, sets, and areas which are controlled by a specific schema. If an installation has multiple data bases, there must be a separate schema for each data base. Furthermore, the content of each data base is assumed to be independent.

A PROGRAM is a set or group of instructions in a host language such as COBOL or FORTRAN. For the purpose of this chapter, a RUN UNIT is an execution of one or more programs.

Data Manipulation Languages (DMLs)

A Data Manipulation Language (DML) is a language used to cause data to be transferred between a run unit (program(s)) and the data base. A DML is not a complete language by itself and is known as a query language by some commercial manufacturers. It relies on a host language to provide a framework for it and to provide the procedural capabilities required to manipulate data.

The User Working Area (UWA) is conceptually a loading and unloading zone where all data provided by the DBMS in response to a CALL for data is delivered. It is also where all data to be picked up by the DBMS must be placed. Each data item included in the subschema will be assigned a location in the UWA and may be referenced by the programs by its name as declared in the subschema.

DBMS Events

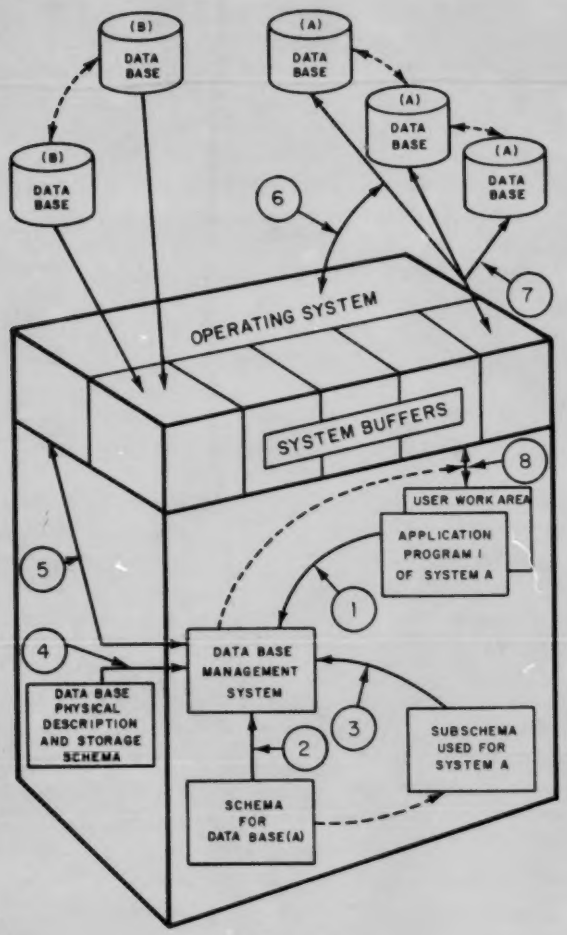
This chapter is not a complete specification for a DBMS. It is intended only as a conceptual training aid for the DP2 in DBMS. This DBMS, as presented in figure 5-6, is for instructional purposes only.

The numbered arrows in figure 5-6 trace a call for data by application program 1 of SYSTEM A. (Calls for data by other programs may be handled concurrently by the DBMS, but this is not depicted in the figure.) The following events (numbered to correspond with figure 5-6) take place, depending on the software system in use, when a program attempts to read a record:

1. Using a DML program 1 of SYSTEM A makes a call for data from DATA BASE (A) to the DBMS.

2. The DBMS analyzes the call and supplements the arguments provided in the call itself with information provided by the schema for DATA BASE (A), and the subschema referenced by program 1.

3. The DBMS obtains the subschema used for SYSTEM A and retrieves the description of the data in question.



78.154

Figure 5-6.–The events that take place when (an) application program(s) reads a record in a system that is interfaced with a DBMS.

4. The DBMS examines the data base physical description and keys the actual physical record to read.

5. On the basis of the call for its services and the information obtained from the schema and subschema, the DBMS requests physical I/O operations, as required to execute the call, from the operating system.

6. The operating system (OS) interacts with the storage media containing the data base.

7. The operating system then delivers the requested data from the actual data base to the system buffers.

8. The DBMS transfers data, as required to fulfill the call, between the system buffers and the UWA of program 1, which originated the call. Any required data transformations between the representation of the data as it appears in the data base (as declared in the schema) and the representation of the data as it appears in a program's UWA (as declared by the subschema) are handled by the DBMS.

The DBMS provides status information to program 1 based on the outcome of its call, for example, error indications. The data in program 1's UWA may be manipulated as required, using the facilities in the host language. The system buffers are shared by all programs serviced by the DBMS. Remember, programs interact with the system buffers entirely through the DBMS.

Schema DDL and Hardware

A schema DDL entry does not include references to a physical device or media space. Thus, a schema written using a DDL is a description of a data base which is not affected by the devices or media used to store the data. The data base may, therefore, be stored on any combination of storage media which is supported in a particular DBMS. Some device (such as magnetic tape), because of their sequential nature, may not take full advantage of the facilities included in a DDL. Such devices are not precluded, however, and may be perfectly adequate for some of the data.

Because of the limited space provided in this rate training manual, the format specifications for a DML and a schema DDL are not presented. The syntax rules for a Data Description Language are similar to those for COBOL and are too technically extensive to include in this chapter. For example, a DDL has a character set, words (programmer supplied), reserved words, key words, names, literal and nonnumeric literal formatting, and many other qualification rules.

Schema/Subschema Data Conversion

Since data description in the subschema is host language oriented, the syntax used in the subschema to describe the characteristics of data items may differ from that in the schema or storage schema. This means that data types which turn out to have the same representation in a given implementation may be described differently in the schema and storage schema than in the subschema. Also, there may be data types defined in the subschema which have characteristics and representations different from those of any schema type, and vice versa. However, any data item description is eligible for inclusion in a subschema for a particular host language subschema data description entry if one of the following conditions is satisfied in the implementation involved:

1. The data item has the same representation both in the data base and in the UWA in that implementation.

2. A conversion procedure has been provided by the implementor.

3. A conversion procedure has been provided by the data base administrator.

The implementor is responsible for defining the correspondence between the schema data types and specifications and the subschema data types and specifications, in terms of the representation of these respective data types in the implementation. An example of a correspondence which might be established by an implementor would be correspondence between coded arithmetic data in the schema and COMPUTATIONAL data in the COBOL subschema.

The implementor might provide special conversion procedures in addition to those in the DBMS for implementing the conversion rules. An example of a case where the implementor might provide a special conversion procedure would be in the interface between the DBMS and data base procedures written in particular host languages. If the DBMS supplies a standard parameter list to data base procedures, the representation of some of the parameter values might not match that of any data type in a particular host language. In this case, the implementor might wish to provide a standard conversion procedure to allow the host language to correctly access such values.

Developers of host language data base facilities may provide rules defining the intended correspondence between data types allowed in their host language subschema DDL and the data types in the schema DDL. Such rules may be specified directly, naming characteristics of subschema data types so that they can be matched with the characteristics of schema data types. Different host languages may define their rules for intended data type correspondence in terms of the closest schema equivalents; e.g., FORTRAN referring to schema TYPE specifications and COBOL referring to schema PICTURE specifications. In this case, the conversion rules specified as part of the schema DDL may be used in determining appropriate conversions involving data types not explicitly mentioned in the host language's defined rules. For example, the COBOL data base facility might specify the intended correspondence between its subschema PICTURE specifications and schema PICTURE specifications. With the correspondence between schema and subschema PICTUREs established, subschema PICTURE specifications may be interpreted as if they were schema PICTURE specifications, and the schema DDL defined conversion rules (which define conversions between schema PICTUREs and other schema data types) then used to determine appropriate conversions between subschema PICTUREs and any schema data type.

Schema and DML

The relationship between a DDL and a DML is the relationship between declaration and procedure. The DDL declarations impose a discipline over the executable code and are to some extent substitutes for procedures written in the DML and the host language.

In order to specify the relationship between DDL declarations and DML commands, a set of basic data manipulation functions must be defined which is independent of the DML and

the host language. Specific commands provided by a particular DML must be resolved into those basic functions. The resolution is defined by the implementor of the DML.

The basic data manipulation functions assumed in these specifications include the functions required to:

1. Select records
2. Present records to the run unit
3. Add new records and relationships
4. Change existing records and relationships
5. Remove existing records and relationships

Schema and Storage Schema

The concept of separate schema and storage schema allows the separation of the logical description of the entire data base from the storage description of the same. This concept is significant from several points of view.

1. A data administrator may design a schema structure consisting of logical records and relationships which sensibly match the totality of applications under implementation or likely to be implemented.
2. Efficiency considerations are separated from logical description by specifying the storage environment and schema to storage schema mappings in the storage schema. Tuning may be carried out by changing the storage schema without alteration to the schema, subschemas, and programs.

The storage schema describes the representation of stored data in device independent terms. The data base may therefore be stored on any combination of storage media which is supported by a particular implementation. The data administrator may allocate media and devices with differing characteristics to suit the command's operational requirements, without alteration to the storage schema.

CHAPTER 6

WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM OPERATIONS COMMUNITY

This chapter provides an overview of the Worldwide Military Command and Control System (WWMCCS) and the computer system that supports WWMCCS commands. It is not the intention of this chapter to cover all existing Honeywell 6000 series configurations and operation procedures for all concerned hardware. It is intended to serve as a management level indoctrination training aid for one of the largest ADP communities within the Navy.

The support and efficient use of WWMCCS is given high priority within the Department of the Navy. Navy and Marine Corps elements of the WWMCCS are maintained to ensure maximum responsiveness to the National Command Authorities (NCA) through the National Military Command System (NMCS).

A command and control system consists of the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces in carrying out the missions assigned. The specific composition of the command and control system depends upon the command's organization and missions, and the types of forces assigned to the command. This composition extends to those operational forces that, due to the nature of their combat employment, must remain directly and immediately responsive to the commander.

NATIONAL COMMAND AUTHORITIES (NCA)

The NCA consists only of the President and the Secretary of Defense, or their duly deputized alternates or successors. The chain of command runs from the President to the Secretary of Defense and through the Joint Chiefs of Staff to the commanders of unified and specified commands.

NATIONAL MILITARY COMMAND SYSTEM (NMCS)

The NMCS is the priority component of the WWMCCS and is designed to support the National Command Authorities (NCA) in the exercise of their responsibilities. The NMCS provides the means by which the President and the Secretary of Defense can receive warnings and intelligence to assist them in making accurate and timely decisions, apply the resources of the military departments, and assign military missions and provide direction to the commanders of unified and specified commands. The NMCS is capable of providing information so that appropriate and timely responses can be selected, directed, and implemented by the NCA. In addition, the NMCS supports the Joint Chiefs of Staff carrying out their duties.

Both the communication of warning and intelligence from all sources and the communication of decisions and commands to the military forces require that the NMCS be the most responsive, reliable, and survivable system available. This requires that the command and control systems within the WWMCCS be configured and operated for effective support of the NMCS, as well as for their specific missions. Interfaces must be compatible; communication links must provide direct connection or real-time relay wherever necessary; computerized data formats must be common; and all details of

system configuration and operation must be as efficient as possible in terms of both effectiveness and utilization of resources.

WORLDWIDE MILITARY COMMAND AND CONTROL SYSTEM (WWMCCS)

The WWMCCS is the worldwide command and control system that provides the means for operational direction and technical administrative support involved in the function of command and control of U.S. military forces. The WWMCCS is composed of:

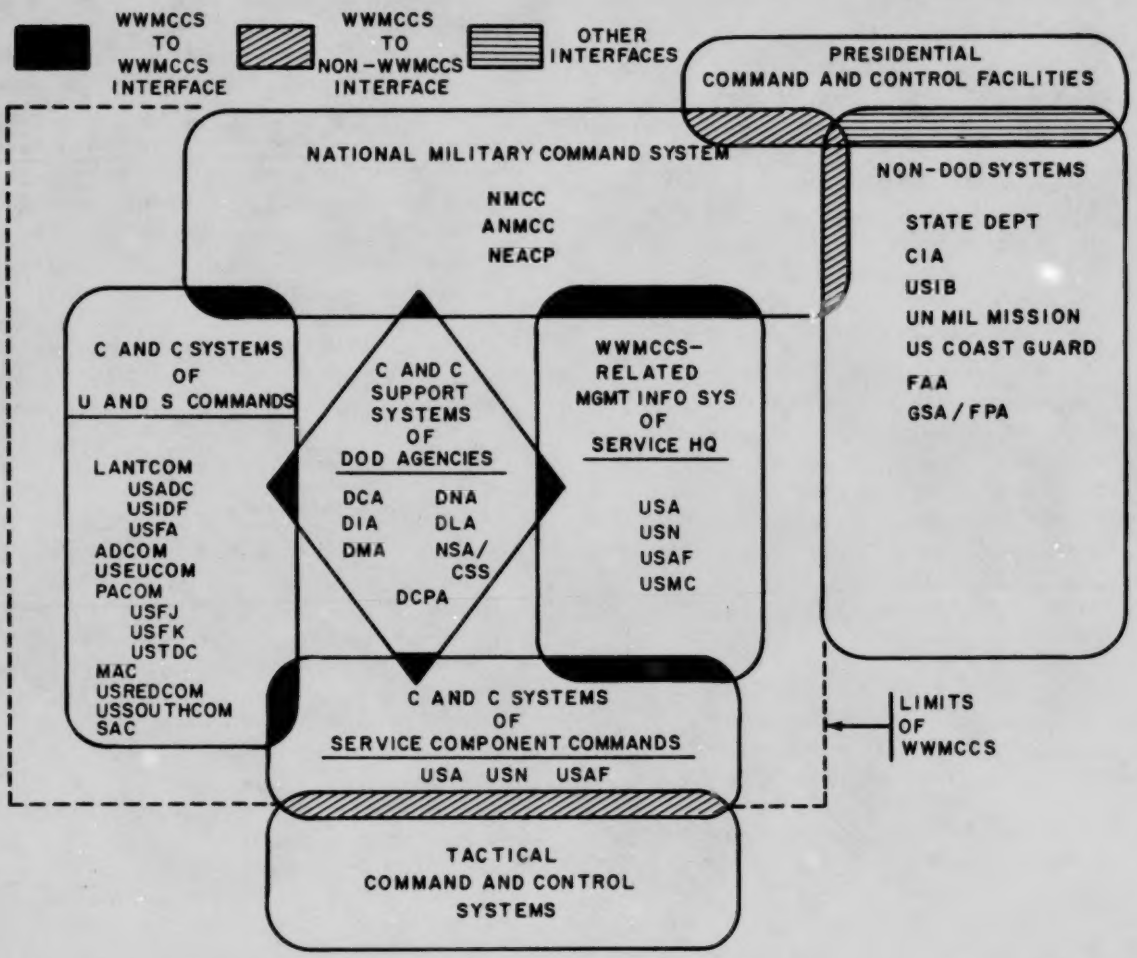
1. The NMCS.
2. The command and control systems of the unified and specified commands; including those command and control systems of subordinate unified commands and joint task forces when such are established and assigned.
3. The WWMCCS--related management information systems of the headquarters of the military departments.
4. The command and control systems of the headquarters of the service component commands.
5. The command and control support systems of Department of Defense agencies. Figure 6-1 is a pictorial representation of the WWMCCS relationships.

Department of Defense (DOD) Directive 5100.30 series provides policy guidance and establishes responsibilities for the management, development, acquisition, and operation of the WWMCCS. It states that the primary mission of the WWMCCS is the support of the NCA. The secondary mission of the WWMCCS is the support of the command and control systems of the unified and specified commands, the WWMCCS-related management/information systems of the headquarters of the military departments, the command and control systems of the headquarters of the service component commands, and the command and control support systems of the Department of Defense agencies.

The effective operation and support of the WWMCCS within the Navy requires that it be recognized as an integrated system, including communications, which extends from the NMCS, through the systems of the commanders of the unified commands and the Chief of Naval Operations, to the command and control systems of the headquarters of the Navy component commanders (CINCLANTFLT, CINCPACFLT, CINCUSNAVEUR, and COMUSNAVSO). Recognition must also be given to the requirement for the WWMCCS to interface through non-WWMCCS Navy command and control systems with those command centers afloat, ashore, or in the air where combat direction is exercised. Efficient command and control requires both the timely, reliable, and secure flow of orders and directions downward through the established operational chain of command. It equally requires the timely, reliable, and secure flow of essential combat information and intelligence laterally and upward to necessary points in the decision process. The WWMCCS, by virtue of its position within the command and control hierarchy, is the cornerstone of any such end-to-end Navy command and control. Its responsiveness to command, as a total system (personnel, equipment, communications, facilities, and procedures), must be ensured.

NAVY HARDWARE/SOFTWARE USERS

The Honeywell 6000 line of hardware and associated software has been selected as the WWMCCS's standard computer system. For Navy users, the hardware system consists of either a single or dual processor 6060 with a variety of peripheral equipment, including card readers and punches, magnetic tape handlers, magnetic disk drives, high-speed printers, and terminal devices such as teletypes, cathode-ray tubes, remote line printers, and the like. Although specific equipment configurations vary in size among installations, hardware types are standard. Because of this diversification in size among installations, it has been necessary to constrain the design of the applications by limiting the resources required for their execution. This has enabled the applications to be implemented at multiple installations. The General Comprehensive Operating Supervisor



78.170

Figure 6-1.–WWMCCS relationships.

(GCOS) operating system, in conjunction with the hardware, is capable of concurrent execution of several programs or program segments within a single processor (multiprogramming) and simultaneous execution of several programs or program segments within two or more processors (multiprocessing). Within such an operational environment, it is necessary to control the allocation of processing resources in order to optimize the utilization and prevent inefficient and ineffective monopolization by a few programs, program segments, or applications. OPNAVINST 5230.12 series sets forth software/hardware applications, operation requirements, and complete management procedures of the WWMCCS new standard computer systems.

The rest of this chapter covers the Honeywell software and hardware being used within the WWMCCS community.

THE WWMCCS HONEYWELL COMPUTER

The Honeywell series 6000 is a family of large-scale, multidimensional information

systems featuring high throughput, optimum use of system resources, and a wide spectrum of user-oriented capabilities.

The series 6000 achieves an exceptionally high level of performance by operating in a total multiprogramming and multiprocessing environment. The system makes full use of its resources through concurrent processing in all dimensions, local and remote batch, direct program access, transaction processing, interactive remote terminal job entry, online document entry, message switching, and time sharing–all using a common data base.

The series 6000 systems are built for maximum uptime. Designed with the latest advances in integrated circuit technology and with improved packaging, the series 6000 systems are compact and easily maintained. Powerful error detection, automatic retry, circuit testers, and comprehensive maintenance panels expedite system diagnosis and help to isolate malfunctions quickly. The total online test and diagnostic routines in the General Comprehensive Operating Supervisor (GCOS) allow temporary deallocation of central system modules, peripherals, communication subsystems for automatic checkout, while normal processing continues in other elements.

GENERAL COMPREHENSIVE OPERATING SUPERVISOR (GCOS)

The GCOS 6000 maintains the status of all system resources (peripherals, memory, and processors) and all user jobs in the system. Using the system scheduler, the allocator queue accommodates a virtually unlimited number of jobs (available disk storage permitting). These jobs can be entered into the system through multiple central and remote devices concurrent with the execution of jobs in the system. The jobs are dispensed to the system according to priorities and resource requirements. The GCOS allocates system resources to jobs in the allocator queue in accordance with the priority of the job, and supervises the concurrent and simultaneous execution of as many programs (up to 63) as the configuration can accommodate. The GCOS also controls the concurrent printing/punching of output from completed jobs. High-priority programs can be expedited by swapping out programs in execution.

The GCOS also provides the programmer with a complete logical approach to problem solution. There are no constraints or unusual programming considerations imposed on the programmers because of the multiprogramming or multiprocessing environment in which the programs are executed. File processing is performed sequentially or randomly at the logical file level; programmers need not be concerned with the physical characteristics and constraints of the peripheral devices used nor with the organization of the file system.

File Management Supervisor (FMS)

The "heart" of a Series 6000 Multidiemensional Information System is a centralized file system of hierarchical, tree-structured design, accessible by programs operating in any of the dimensions. Catalogs and files are secured by passwords and permissions. File access is controlled by the FMS. Several programs can read and/or update a file concurrently. The FMS performs vital protective and restorative file monitoring and resource control functions in all processing modes. Files are automatically sustained in a readily usable and extremely reliable condition. A unique design feature of the file system allows maintenance (repacking) routines to be "cleaning up" a portion of the file system while production routines in concurrent operation are accessing other portions of the system.

Batch Processing

The GCOS 6000 provides a flexible, high-throughput batch processing environment. Up to 63 programs can be in concurrent execution. Incoming jobs are classified into a number of separately defined job streams, permitting users to control their own priorities. Roll-out, roll-in capabilities allow for fast response to high-priority jobs or transactions. Batch jobs may be submitted from any local input device or remote terminal at any time, without operator intervention.

Remote Processing

Concurrent remote processing capabilities can be added to the Series 6000 systems by including one or more DATANET 30, DATANET 305, or DATANET 355 Front-End Network Processors (FNP) in the configuration. Each FNP permits a variety of terminal, transmission rate, and processing options. Remote processing capabilities include remote batch, direct program access, transaction processing, message switching, and time sharing. The GCOS remote access uses a reactive terminal interface which provides direct terminal access (through the FNP) to the information system and to the common file system, facilitating the development of "online" terminal applications.

Transaction Processing

The transaction processing system opens the door to online, real-time data processing. Transactions (messages representing events in the users environment) can be entered via remote terminals. The transaction processing system interprets the transaction code contained in the message and calls the necessary application programs into execution to process the message. The output or acknowledgment will be returned to the designated terminal.

Time Sharing

The time sharing executive, which utilizes the reactive terminal interface, provides the WWMCCS Series 6000 installations with concurrent time sharing. Language capabilities include FORTRAN, a scientific-oriented language; BASIC, an easy-to-use, probem-solving language; and a powerful text-editing package to create, update, and obtain formatted text. Full upper/lower case ASCII character handling is provided. Many other languages and systems such as ALGOL, JOVIAL, ABACUS, and a time-sharing library of applications are also provided. Catalog structuring, file protection, file sharing, access control, and source/object file storage capabilities are provided through the file system. The time-sharing batch capability permits time-sharing users to create and initiate batch mode programs and to scan or receive the batch output–all from a time-sharing terminal. In addition, the structure of the Time Sharing Executive and the integration of time-sharing files in the file system facilitate user extension of the time-sharing system to provide further remote processing capabilities.

Interactive Remote Job Entry

The interactive remote job entry includes an interrelated set of time-sharing subsystems and batch programming that together provide a powerful capability for full batch dimension programming from a remote terminal such as a teleprinter. Turnaround time and programmer productivity for even very large programs are greatly improved.

On-Line Document Handler

The Series 6000 Document Entry Subsystem (DS 6000) is a combination of hardware and software and is designed to perform the vital processing of magnetically and optically encoded documents. The DES 6000 modular design allows for great flexibility in meeting the changing document entry requirements during the processing cycle of each day. High-speed, high-capacity document operation can proceed within the Series 6000 environment concurrently with other normal dimensions controlled by the GCOS, without the restrictions that document entry/sorting normally imposes upon an operating system.

Message Switching

Message switching adds yet another dimension to multidimensional GCOS. The comprehensive message switching capability of the Network Processing Supervisor (NPS) with the DATANET 355 Front-End Network Processor allows data exchange between terminals, between terminals and the information processor, and between the information processor and terminals. The message switch system operates in store and forward mode, receiving each message completely and storing it in a journal before

forwarding it to the addressed destination(s). The message switching dimension control is entirely within the DATANET 355.

Total Online Testing System (TOLTS)

The Total Online Testing System is composed of four major subsystems for peripheral, communications, main frame, and remote testing. This online testing system is part of a total maintenance and recovery concept. Eight concurrent diagnostic programs can operate with user programs under the GCOS.

HARDWARE OVERVIEW

Honeywell Series 6000 systems provide processing and input/output capabilities across a wide performance range. The systems are tailored to the specific workload and processing environment of the installation through the selection of the appropriate system model, and by the configuration of central system modules and peripheral devices. System models are differentiated by the speed of the central system components.

With a system model, further performance flexibility is possible through "functional modularity" or the selection of central system modules to match the work load needs of the installation. The General Comprehensive Operating Supervisor (GCOS) is the same for all models and configurations and provides multidimensional processing capabilities from the smallest to the largest system.

Functional Modularity

Series 6000 multidimensional systems employ a unique design concept which provides complete flexibility in configuring the precise blend of processing, memory input/output, and communications resources to perform efficiently any given scientific/data processing workload mix. This concept also facilitates major system extension without reprogramming or conversion.

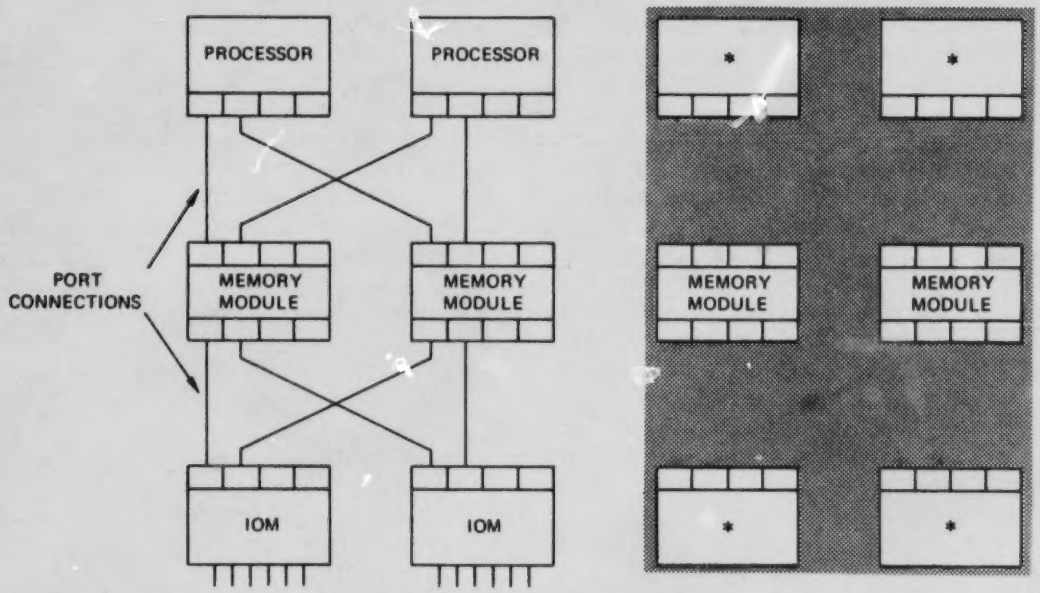
The major system functions of processing, memory, input/output, and communications control have been separated into the following discrete functional modules:

1. Memory Modules–To provide the required amount of directly addressable primary memory.
2. Bulk Store Subsystem Modules–To provide the required amount of secondary memory.
3. Processor Modules–To provide the required amount of computational capability.
4. Input/Output Modules–To control the required level of data input/output between memory and the peripheral and communications subsystems.
5. Front-End Network Processor Modules–To control data communications functions and provide service to remote users.
6. Data Entry Controller Module–To provide on-line paper document entry.

Multiple modules of each type may be configured on an information system to match the processing, memory size, memory access, and data input/output requirements of an installation workload. This modular construction results in configurations that are tailored to the precise needs of an installation. System growth is readily accomplished by adding the appropriate modules as they are needed. Added reliability is a by-product of system extension, since all modules of a given type are identical and can provide backup for each other.

The operating system (GCOS) automatically adapts itself to control any standard equipment configuration. No system generation is required. One version of one operating system supports the smallest to the largest configuration.

Figure 6-2 illustrates the way the central system modules are interconnected to provide a high degree of functional modularity and backup capability. The solid-line figures represent a configuration consisting of two processor modules, two memory modules, and two input/output multiplexer (IOM) modules. Every processor and IOM connects through ports to each memory modules; these connections permit access to the full range of



NOTES: PORT CONNECTIONS ARE MADE FROM *EVERY* MEMORY MODULE TO *EVERY* ACTIVE MODULE.

*ANY OF THE FOLLOWING MODULES: PROCESSOR, IOM, DATANET 355 FNP, DATA ENTRY CONTROLLER, OR BULK STORE CONTROLLER.

78.170.1

Figure 6-2.–Functional Modularity.

processors, memory, and peripherals. The broken lines represent expansion capabilities. The system grows by adding more processors, memory, input/output multiplexer modules, or Front-End Network Processors with no user conversion.

Memory Module

Each memory module is composed of a system controller and associated memory units. Series 6000 systems are "memory-oriented," permitting processor and IOM functions to execute asynchronously and simultaneously. The memory module has neither program execution nor arithmetic capability, but acts as a passive system component. It serves the processor, I/O multiplexer, and DATANET 355 FNP, data entry controller, and bulk store subsystem modules which call upon the memory module to save or retrieve information or to communicate with other system components.

Each access in the memory module is composed of eight 9-bit bytes plus 2 parity bits. For purposes of memory protection in multiprogramming, the memory is organized into 1024-word (94096-byte) blocks. Each memory module can contain up to 262,144 words (1,048,576 bytes) or (256 blocks) of memory.

The system controller has up to 8 ports for connection to active modules and also contains 32 program interrupt cells. The eight ports have "wired-in" positional priority in the order of their numbers (0 . . . 7); thus, simultaneous requests are serviced in a predetermined manner.

Increased system throughput is achieved by operating the memory module and associated memory units on a 72-bit parallel basis. This corresponds to 2 instructions, 2 data words, 8 data bytes, 12 data characters, or 1 double-precision fixed- or floating-point number.

Systems with more than one system controller provide additional effective information rate, since each system controller operates independently and its functions can be overlapped with those of other system controllers. Additional overlap is provided by the address interleaving feature of the Series 6000 systems. Address interleaving considerably reduces the probability of the same memory unit being accessed in succession. Furthermore, the processor and system controller are especially designed to utilize memory accesses of two memory units in rapid succession. These two factors contribute to the higher access rates and effective memory cycle times of the Series 6000 systems. For example, Models 6070 and 6080 can have each of four memory units provide a complete memory cycle (read/write) of two full 36-bit words, or eight 9-bit bytes within a single basic cycle time of 500 nanoseconds—an effective rate of 16 nanoseconds per byte.

Processor Module

Series 6000 systems are highly modular, allowing the system configuration to be matched to the workload mix. The Extended Instruction Set (EIS) processor is particularly well suited for heavy workloads, while the other models handle mixed workloads of business and scientific jobs.

Each processor module has full program execution capability and conducts all actual computational processing (data movement, arithmetic, logic, comparison, and control operations) within the information system. The processor, which communicates only with the system controller(s) and associated memory, consists of an operations unit and a control unit. The operations unit executes arithmetic and logic operations; the control unit performs instruction fetching, address preparation, memory protection, and data fetching/storing. Both units operate with relative independence and maximum overlap to provide the highest possible rate of instruction execution on the faster models.

The processors contain several special features that make significant contributions to the exceptional multiprogramming, high througput, and rapid turnaround capabilities of the information systems. These features are under the control of the GCOS, which maintains automatic supervision and complete control of the multiprogramming/multiprocessing environment. These features are:

DUAL-MODE OPERATION.—The processor has two modes of operation—master and slave.

1. The master mode, reserved for the GCOS, allows unrestricted access to all of memory, permits initiation of data input/output operations through the IOM(s), and permits the setting of control registers.

2. The slave mode, used for the execution of all user programs, is also used by the GCOS when appropriate. Slave mode operation restricts memory references to assigned program boundaries and causes all memory references to be relative to a base address register (BAR). Program execution time is strictly limited by a timer register. Also, program execution is limited to a subset of the instruction repertoire—control operations (such as input/output operations or setting the BAR and timer registers) cannot be executed in the slave mode.

Dual-mode operations provides effective operating control and protection of the information system's multiprogramming environment to the GCOS.

BASE ADDRESS REGISTER (BAR).—Each processor contains a base address register, which performs both address translation and memory protection functions in the slave mode of operation. (The BAR is not used in master mode processing.) The BAR is set by the GCOS prior to transferring control to a slave program. It contains the beginning address of the program (absolute) in memory and the number of 1024-word or 4096-byte blocks assigned to the

1024-word or 4096-byte blocks assigned to the program. Program memory is logically and physically contiguous.

During slave mode execution, each memory address developed by a program is checked to ensure that the address is within the area of memory assigned to the program. If the developed address is within the program's area, the address is added to the beginning address value in the BAR to develop the true address, and the memory access is performed. If the address developed by the program is outside the area of memory assigned to the program, control automatically reverts to the GCOS for appropriate action.

An important attribute of the BAR is its ability to move user programs in memory without address relocation merely by establishing a new BAR setting. This feature is used for program swapping and memory compaction.

TIMER REGISTER.–Each processor contains a timer register, which initiates a program interrupt at the end of a preestablished interval of time. The interval is set by the GCOS prior to giving control to a slave program. (The timer register can be set in master mode only.) The timer register is used by the GCOS to time programs for automatic termination, to prevent programs from monopolizing a processor, and to provide detailed accounting information on processor and peripheral use time.

PROCESSOR FAULTS.–Sixteen special processing status conditions, termed "faults", cause interruption of sequential instruction execution and transfer of control to 1 of 16 discrete fault vector locations for appropriate action by the GCOS. Faults provide program control (e.g., arithmetic overflow) and system control (e.g., timer runout or an attempt to reference outside of memory limits), and call for operating system services (e.g., master mode entry).

EXTENDED INSTRUCTION SET (EIS).–EIS models have processor instructions well suited for workloads with a predominance of business rather than scientific work. The EIS processor has all of the instructions of the other models plus many business-oriented features, inluding decimal arithmetic, powerful editing, mixed-mode operations, address registers, and extended instruction format (multiword instruction) with two or three addresses. For example, a single COBOL statement can be performed by a single instruction on the EIS processor but would require several instructions on a conventional processor. This not only reduces the memory required but also the execution time.

Input/Output Multiplexer (IOM)

Each IOM module operates essentially as a stored-program device controlled by, and sharing memory accesses with, the processor modules. Data transfer operations are initiated by the GCOS in the master mode. (Data transfer operations cannot be initiated by a program in the slave mode.) Peripheral device operations are controlled by processor-prepared control word lists stored in the communications region in memory (referred to as "IOM mailboxes"). Data transfer operations are performed asynchronously with program processing with minimum interference between the processor and input/output.

Each IOM module in any configuration is directly coupled to each memory module, providing direct access to all of memory. Data transfer operations are controlled by lists of data control words (DCW), which specify the areas of memory to/from which data is to be transferred. These DCW lists allow data to be gathered from, or distributed to, noncontiguous locations in memory.

Memory protection of data transfers is performed in much the same manner as in the processor. The BAR setting of the program requesting the I/O is inserted as part of the required instructions in the IOM mailboxes. Each DCW processed by an IOM is checked for address limits. If an out-of-bounds address is detected, the transfer is not performed and an appropriate interrupt is generated to the control processor. IOM communication with the processor is effected through the IOM

mailboxes and through four discrete types of interrupts to 1 of 32 present interrupt vector locations. All data transfer and peripheral status conditions of interest are signaled to the control processor via the interrupt mechanism to maximize peripheral utilization and program throughput.

In Series 6000 information systems, the input/output multiplexer (IOM) is the coordinator of all input/output operations between the complement of peripheral subsystems and system controllers. The input/output multiplexer operates essentially as a hard-wired program device controlled by, and sharing memory with, a processor. Data transfers between a peripheral device and memory are accomplished by the IOM while the processor runs the jobs. Peripheral devices are controlled by processor-prepared control words stored in the memory.

Significant features of the input/output multiplexer include:

1. Complete memory protection for all input/output multiplexer data transfers.
2. Total awareness of the number, types, and states of up to 24 I/O subsystems per IOM.
3. Hardware/software integration resulting from control programs designed to take full advantage of equipment features.
4. Ability to interrupt processor operations.
5. Scatter/gather of noncontiguously stored I/O program data.
6. A special I/O processor for peripheral channel management.
7. Maximum data transfer capacity of 6 million characters per second.
8. Maximum single-channel data transfer capacity of 1.3 million characters per second.
9. Simultaneous operation of peripheral subsystems in a wide range of equipment configurations.
10. Communications with multiple independent system controllers.
11. Scratchpad storage for control words on some models.
12. Six special channels to provide for specific system functions, including new test and diagnostic aids.

REMOTE INPUT/OUTPUT OPERATIONS

Data communications systems, essential to many existing and future computer applications, are integral parts of the Series 6000 Information System. The GCOS permits multiple remote terminals and computers at widely separated locations to communicate with the system. One-way or two-way communication over common and private carrier lines, coaxial cables, or via microwave transmission can be channeled through a selection of DATANET Front-End Network Processors (FNPs).

Remote Processing Capabilities

Remote processing capabilities are provided in many modes of the Series 6000 Multidimensional Information System:

1. Remote batch
2. Direct program access
3. Time Sharing
4. Transaction processing
5. Message switching
6. On-line document entry

Through these dimensions or modes of operation, the remote terminal user has access to the full capabilities of the system.

The GCOS takes advantage of features within the information system to enable the user (in various data communications applications) to achieve:

EFFECTIVE REMOTE DATA PROCESSING.–The multiprogramming environment can include a large number of users in both local and remote locations with diverse processing needs.

RADICAL REDUCTIONS IN TURNAROUND TIME.–Total turnaround time, the period between the submission of a job for processing and the receipt of the desired output, is a function of several factors:

–Input time
–Time spent in awaiting processing
–Actual processing time
–Time spent in awaiting output
–Actual output time

Through the use of multiple local and remote input/output devices, simultaneous processing and input/output operations, and automatic job interrupts, the nonproductive waiting time and output time can be reduced to a level commensurate with the high-speed processing capabilities of the information system.

Standard terminals accommodated by the GCOS include the:

1. Honeywell Series 100 remote batch computers
2. Honeywell VIP 765/775/785/786/7705 visual display terminals
3. Teletype Models 33, 35, and 37 Teleprinters
4. GE TermiNet 300 or Honeywell SRT301 Teleprinter
5. IBM 2741

The three communications processors providing the network processing of Series 6000 Multidimensional Information Systems are the:

1. DATANET 355 Front-End Network Processor
2. DATANET 305 Front-End Network Processor
3. DATANET 30 Front-End Network Processor

DATANET 355 Front-End Network Processor

The DATANET 355 is a high-performance, stored-program FNP designed to match the large-volume communications needs of the Series 6000 Multidimensional Information Systems. The DATANET 355 FNP features total integrated circuit logic construction and a memory size of 16,384 or 32,768 words (18 bits or 2 bytes per word) with a cycle time of one microsecond. The DATANET 355 FNP accommodates data of variable word lengths–6, 9, 18, or 36 bits. All data word lengths are individually addressable to allow highly efficient processing of tabular data. Ninety-eight instructions in an 18-bit format are provided, with one single-address instruction per word. Three index registers and multilevel indirect addressing, with indexing at all levels, give an addressable storage capability of up to 32,768 words.

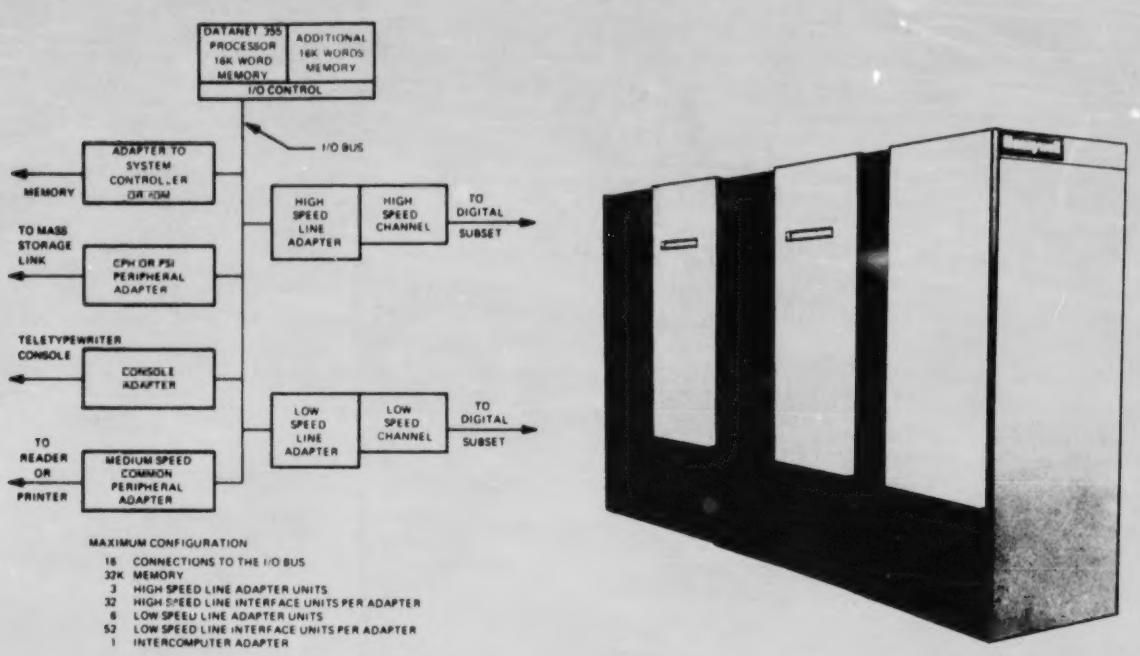
The input/output is designed to facilitate efficient realtime concurrent servicing of multiple terminals and peripheral devices. Up to 16 adapters can be provided to accommodate a total data transfer rate of up to 500,000 words per second (with 6, 9, 18, or 36 bits per word). Sixteen levels of priority interrupt, with 16 sublevels per level and corresponding interrupt masks, are provided.

The system organization of the DATA NET 355 FNP follows the pattern of the Series 6000. The DATANET 355 is a storage-oriented computer with its own independent memory, processor, and input/output modules. These three basic DATANET 355 modules are independently timed and operate asynchronously with each other. The processor and the input/output controller (which are active units) process data at their own rates and request cycles from the storage module (a passive unit) as the need arises. Only when the processor executes certain input/output instructions must the processor and the input/output controller of the DATANET 355 communicate with each other.

COMMUNICATIONS SUBSYSTEM.–The DATANET 355 FNP, as a module of the Series 6000 Multidimensional Information System, is capable of simultaneously handling up to 200 teleprinter users (110 to 300 bps), or 32 remote batch users (voice-grade or broadband), or 32 CRT subsystems (voice-grade), or an appropriate mix of these three classes. (See fig. 6-3)

The DATANET 355 FNP consists of a DATANET 355 processor with the following input/output adapters:

1. The DATANET 355 Intercomputer Adapter (ICA) with up to four ICA ports to interface with the Series 6000 system controllers or a direct interface adapter to interface with an IOM
2. Up to three High-Speed Line Adapter (HSLA) units


DATANET 355 PROCESSOR 16K WORD MEMORY
ADDITIONAL 16K WORDS MEMORY
I/O CONTROL
I/O BUS
ADAPTER TO SYSTEM CONTROLLER OR ROM
MEMORY
HIGH SPEED LINE ADAPTER
HIGH SPEED CHANNEL
TO DIGITAL SUBSET
TO MASS STORAGE LINK
CPH OR PSI PERIPHERAL ADAPTER
TELETYPEWRITER CONSOLE
CONSOLE ADAPTER
LOW SPEED LINE ADAPTER
LOW SPEED CHANNEL
TO DIGITAL SUBSET
TO READER OR PRINTER
MEDIUM SPEED COMMON PERIPHERAL ADAPTER
MAXIMUM CONFIGURATION
16 CONNECTIONS TO THE I/O BUS
32K MEMORY
3 HIGH SPEED LINE ADAPTER UNITS
32 HIGH SPEED LINE INTERFACE UNITS PER ADAPTER
6 LOW SPEED LINE ADAPTER UNITS
52 LOW SPEED LINE INTERFACE UNITS PER ADAPTER
1 INTERCOMPUTER ADAPTER

78.171

Figure 6-3.–DATANET 355 System configuration.

3. Up to six Low-Speed Line Adapter (LSLA) units

4. A console adapter for connection of a teletypewriter console

5. An adapter link to Series 6000 mass storage

HIGH-SPEED LINE ADAPTER (HSLA).–The HSLA is a multiline communications controller with up to 32 concurrently operating lines. The following types of channels are available on the HSLA:

1. Broadband (19,200 to 50,000 bps)

2. General purpose (75 to 9,600 bps)

3. Dual synchronous (2,000 to 9,600 bps)

4. Dual asynchronous (110 to 1,800 bps)

These channels are modular in design and can be configured in any combination not to exceed 16 terminals total per HSLA (32 lines). Because of its flexibility, the HSLA and its channel offering can interface with every type of remote terminal supported on the Series 6000 systems.

LOW-SPEED LINE ADAPTER (LSLA).–The LSLA provides the primary facility for connecting low-speed terminals to the DATANET 355 FNP. Up to 52 terminals at 110 bps, or 26 terminals at 134.5/150 bps, or 17 terminals at 300 bps, or a combination of these can be connected to a single LSLA. The LSLA operates with low-speed terminals in either the full- or half-duplex mode for asynchronous data transfer. The LSLA operates on the principle of time-division multiplexing, developing a message frame composed of a number of 8-bit characters called time slots, each time-slot containing one complete character associated with a particular terminal.

	Model 6030/6040	Model 6050/6060	Model 6070/6080
Max. No. of Processors	1	4	4
Max. No. of DATANET FNPs or DEC6000s	3	3	3
Max. Memory Size (in 36-bit words)	262,144	524,288	1,048,576
Max. Memory Size (in 9-bit bytes)	1,048,576	2,097,152	4,194,304
Memory Cycle Time (8 bytes)	1.2	1.2	0.5
Max. No. of IOMs	1	4	4
Max. Transfer Rate per IOM (bytes/sec)	0.8 or 2.0M	2.3M	4.0M
Max. Transfer Rate per IOM (char/sec)	1.3 or 2.8M	3.7M	6.0M
No. of Data Channels per IOM	16	24	24
Peripheral Capacity (subsystems)	16	24	24
I/O Compute Simultaneity	16	24	24
Programmable Registers	49/57	49/57	49/57
Floating Point	Yes	Yes	Yes
Memory Protect	Yes	Yes	Yes
Hardware Radix Conversion	Yes	Yes	Yes
Interleaving	No	Yes	Yes
Instruction Overlapping	No	Yes	Yes
Instructions per Second (max.)	340,000	550,000	1,400,000

Figure 6-4.—Series 6000 characteristics.

SERIES 6000 CHARACTERISTICS

Figure 6-4 gives the general characteristics of the various Series 6000 models. Models 6040, 6060, and 6080 have the Extended Instruction Set (EIS) processors, while Models 6030, 6050, and 6070 do not. The basic batch-only system in figure 6-5 contains a single processor, a single system controller, and a single IOM with its peripherals, while the mutidimensional system requires more memory, possibly two or more system controllers, and a DATANET 355 Front-End Network Processor as shown in figure 6-6. The FNP is essential for all dimensions of the systems except local batch.

Figure 6-7 illustrates the central configuration of a multiprocessor system. Fundamental to Series 6000 operation is the fact that all active modules (processors, IOMs, DATANET 355 FNPs, DEC6000s and bulk store controllers) connect to all system controllers, and thus have common access to memory and to the common data base. These connections permit the GCOS to assign work to the available resources.

Although figure 6-7 shows only two processors, one IOM, and one DATANET 355

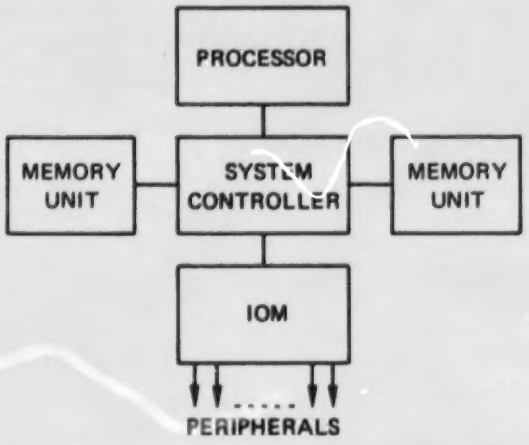
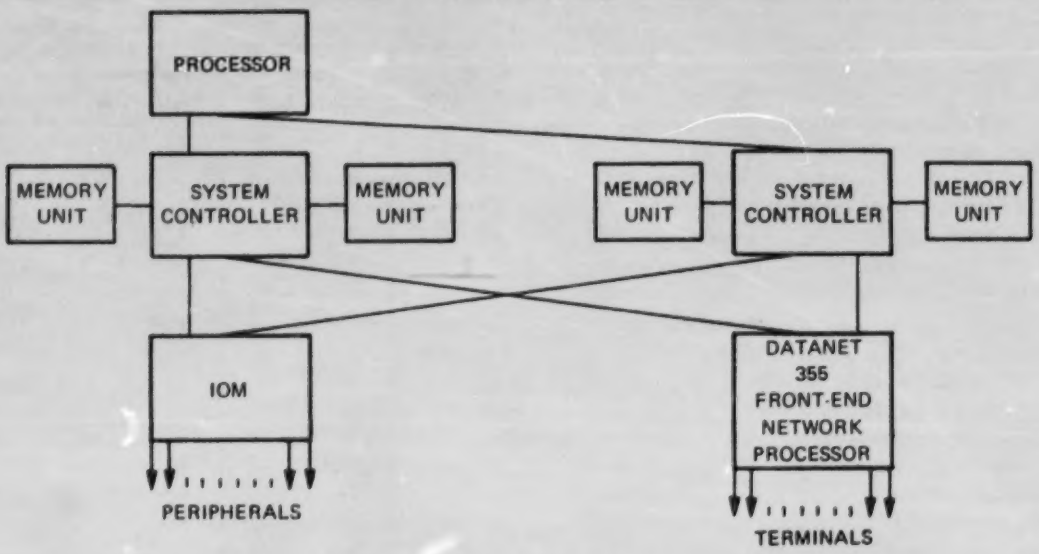


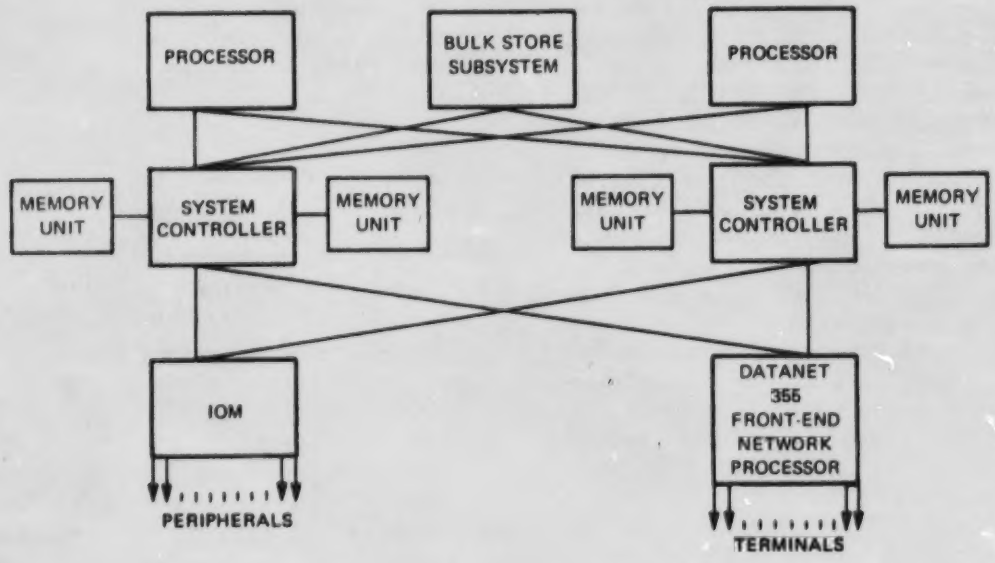
Figure 6-5.—Basic system.



78.172

Figure 6-6.—Multidimensional system.

FNP, the system allows as many as four processors, four IOMs, three DATANET 355 FNPs/DEC6000s, and two bulk store controllers, subject to the additional theoretical restriction of eight total active modules. It is unlikely that eight or more active modules would be required to perform the work load of a WWMCCS. Along with the functional modularity of the hardware configuration, there is complete program compatibility so that any



78.173

Figure 6-7.—Multiprocessor multidimensional system.

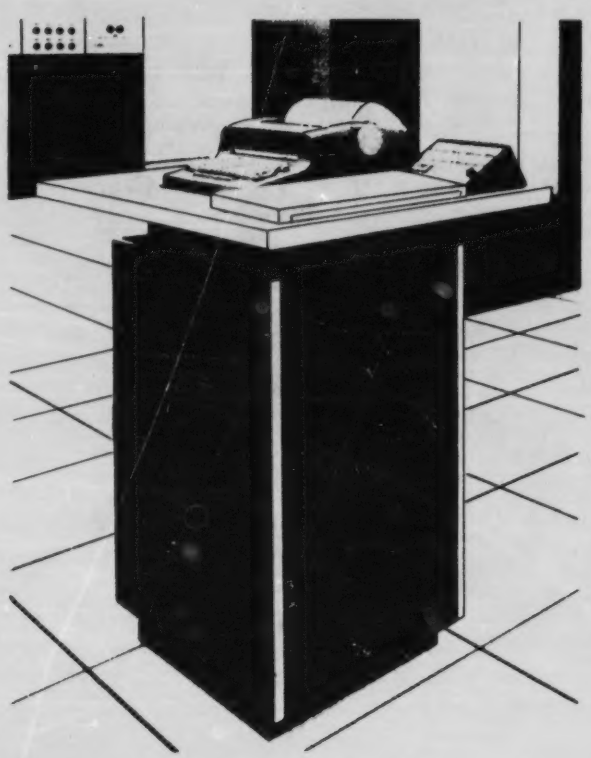
141

program that is capable of running on one configuration can run on any other configuration (except for EIS programs, which must run on an EIS system).

Peripheral Subsystems

All peripheral subsystems communicate with Series 6000 Multidimensional Information Systems through an input/output multiplexer (IOM). There are two standard interfaces available on the IOM for the connection of peripheral controls–the common peripheral interface (CPI) transfers data in excess of 650 thousand characters per second, while the peripheral subsystem interface (PSI) is capable of transferring data in excess of 1.3 million characters per second. These interfaces support a variety of peripheral device controls, such as magnetic disk and tape controls, card readers, printer and punch controls, and data communications processors.

The GCOS issues commands to the peripherals through the IOM. Peripheral devices can also request action by transmitting special interrupts to the GCOS. Representative peripheral subsystems that can be utilized with Series 6000 Multidimensional Information Systems are described later in this chapter.



78.174

Figure 6-8.–Control console.

Control Console

The primary function of a control console is to provide for direct communication between the operator and the GCOS. The master console is a freestanding unit of suitable operator working height that connects to a common peripheral interface channel of the IOM; the console is controlled just as a peripheral subsystem. (See fig. 6-8.) Significant processor and system controller functions are displayed on the system status display panel, keeping the operator constantly informed of running status. The status display panel contains the following indicators and controls:

1. SYSTEM READY light
2. OPERATOR ATTEN light and switch (attention)
3. DIS light (processor waiting)
4. INSTRUCTIONS EXECUTED/SECOND indicator
5. CONSOLE READY light
6. MASTER MODE light
7. SLAVE MODE light
8. EMERGENCY POWER OFF switch

The console includes an input/output typewriter that accepts input data via keyboard entry and transmits the data to the input/output multiplexer. Output messages from the IOM are printed at 15 characters per second (nominal). An operating routing within the GCOS provides responses to operator requests through the typewriter.

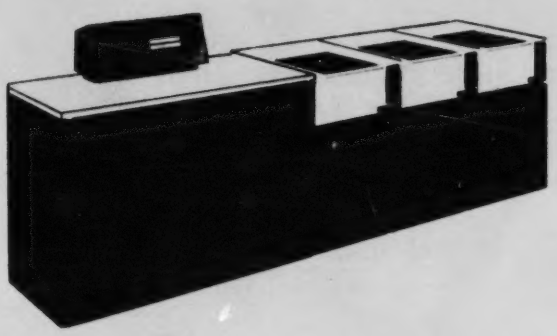
DSS181B Disk Storage Subsystem

The type DSS181B disk storage subsystem provides medium size, modular, auxiliary system storage for online, direct-access programming. (See fig. 6-9.) At some WWMCCS sites the DSS181 and DSS191 disk storage subsystems are being replaced by the DSS450 and DSS451 disk storage subsystems.

STORAGE CAPACITY–Each removable disk pack stores 27,648,000 characters or 18,432,000 bytes. Online storage per disk subsystem ranges from a minimum capacity of 82 million characters or 55 million bytes (3 operating spindles) up to 442 million characters or 294 million bytes (16 operating spindles) of online direct-access storage.

DISK AND RECORD LAYOUT–Data is grouped in a total of 72,000 continuously addressable sectors of 384 characters each. A total of 360 sectors (138,240 characters) are accessible in each actuator position or cylinder.

Bits per character:	6
Bits per byte:	9
Characters per sector:	384
	(256 bytes)
Sectors per track:	18
Characters per track:	6,912
	(4,608 bytes)
Tracks per cylinder:	20
Characters per cylinder:	138,240
	(92,160 bytes)
Cylinders per disk pack:	200 plus 3 spares
Characters per disk pack:	27,648,000
	(18,432,000 bytes)



78.175

Figure 6-9.–DSS181 disk storage subsystem.

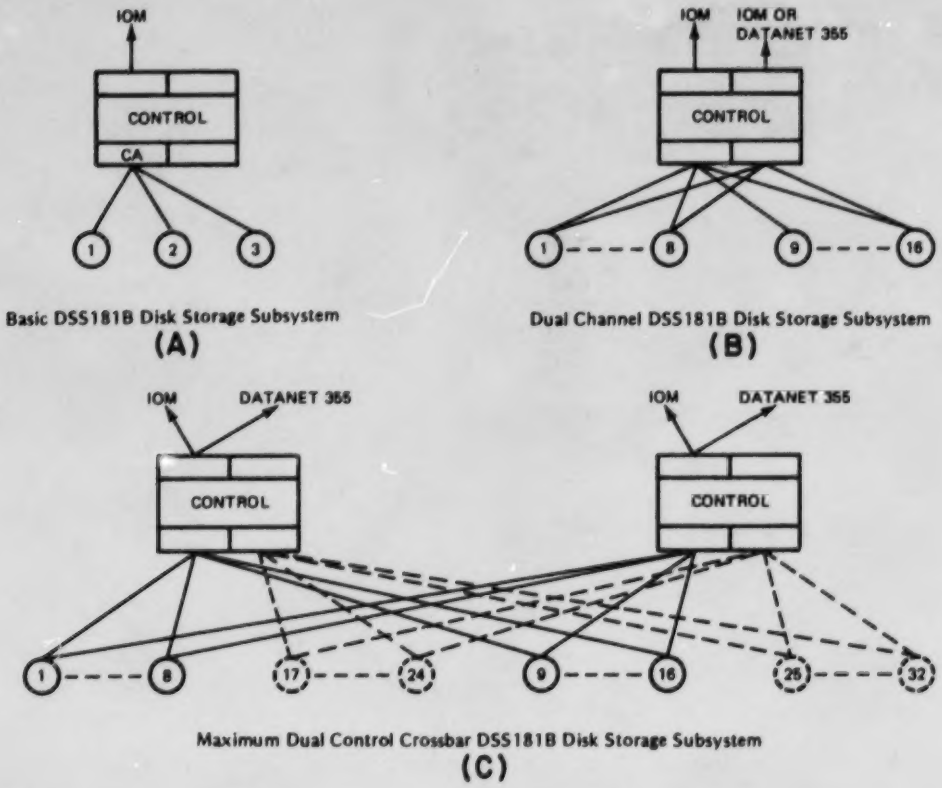
CONTROL–The control handles up to 16 online disk pack drives. Command decoding, data checking features, and data control are provided in the control hardware. (See fig. 6-10A.)

DUAL CHANNEL OPTION–Provided in the control and drives is the option for dual, simultaneous cross barred channels. (See fig. 6-10B.) Dual simultaneous channels provide higher throughput and greater availability of data. This option permits multiaccesses to the device level. Each channel is capable of simultaneous command and data transfers to different disk pack drives while overlapping seeks on all other drives.

SWITCHED CHANNEL OPTION–Nonsimultaneous channels permit sharing of the disk storage between the central system and the Front-End Network Processor.

DUAL CONTROL SUBSYSTEM–Two single-channel controls may be connected into a cross-barred subsystem to provide higher throughput to a larger data base (32 drives) and greater data availability by independent access to all 32 drives through either channel. (See fig. 6-10C.)

BLOCK COUNT–The hardware block count provides protection where multiple files share the same cylinder. Such blocks, or sectors, are specified by the processing system, and the limit



78.176

Figure 6-10.–DSS181B configurations.

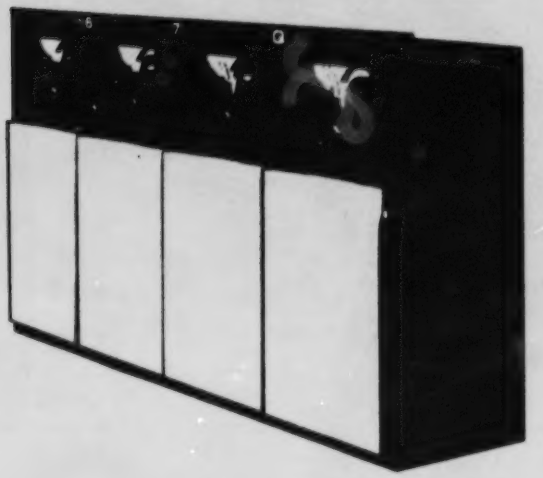
can vary from one up to the maximum number of sectors within a cylinder. Configuration Features:

1. Maximum dual-channel crossbar with 32 disk-pack drives provides a capacity of 884 million characters or 589 million bytes.
2. Dual channel–optional.
3. Additional (switched) data channel–optional.
4. Dual-control crossbar–optional.
5. Basic configuration consists of control and three disk-pack drives.
6. Expandable up to 221 million characters (147 million bytes) by adding up to five additional disk-pack drives.
7. Additional drive electronics in control provide capability for increased capacity of up to 442 million characters or 294 million bytes (16 disk-pack drives).

Magnetic Tape Subsystems

The data medium is half-inch wide, magnetic-oxide plastic tape, up to 3,200 feet long. Data formats are binary (standard) and special decimal. Checking features include:

Transfer Timing	Missing Character
Blank Tape Read	Longitudinal Parity
Transmission Parity	Bit Detected During Erase
Lateral Parity	Cyclic Redundancy



78.178

Figure 6-11.—Magnetic tape unit.

The average rewind speed is 500 ips on the MTH500 series; 300 ips for other tape handlers. Features of the Magnetic Tape subsystems in figure 6-11 include:

1. Either single-channel or dual-channel control of tape units.
2. Densities of 200/556/800/1600 BPI.
3. Program or operator control of recording density.
4. Special decimal mode which provides campatibility with non-Honeywell tape systems.
5. Dual-gap read-write heads for read-after-write checking.
6. Tape control buffering during data transfers.
7. File protection through use of a write-permit ring.

Type Number	Tape Tracks	Tape Speed (ips)	Density (bpi)	Transfer Rates (thousands per second) 6-bit Character	8-bit Bytes
MTH200	7	37.5	200/556	7.5/21	–
MTH300	7	37.5	200/556/800	7.5/21/30	–
MTH201	7	75	200/556	15/42	–
MTH301	7	75	200/556/800	15/42/60	–
MTH372	7	150	200/556	30/83	–
MTH373	7	150	200/556/800	30/83/120	–
MTH404	9	75	200/556	20/56	15/42
MTH405	9	75	200/556/800	20/56/80	15/42/60
MTH492	9	150	200/556	40/111	30/83
MTH493	9	150	200/556/800	40/111/160	30/83/120
MTH501	7	75	200/556/800	15/42/60	–
MTH502	9	75	200/556/800/1600	20/56/80/60	15/42/60/120
MTH504	7	125	200/556/800	25/70/100	–
MTH505	9	125	200/556/800/1600	33/93/133/267	25/70/100/200

Figure 6-12.—Magnetic tape unit characteristics.

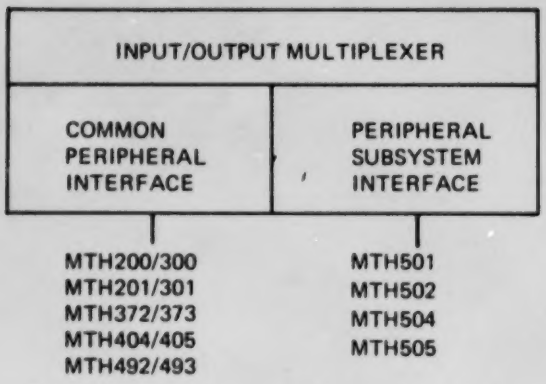


Figure 6-13.–Magnetic tape interface.

Additional features of MTH500 series include:

1. In-flight error correction–1600 BPI
2. Canister loading
3. Automatic threading
4. Power window

MODULARITY AND FLEXIBILITY.–A full range of tape handlers with various speeds, densities, and transfer rates is available with Series 6000 magnetic tape subsystems (fig. 6-12). All of the magnetic tape controls, except the controls for MTH500 Series handlers, connect to the IOM via common peripheral interface channels (fig. 6-13). The controls for MTH500 Series handlers connect to the IOM via peripheral subsystem interface channels, permitting higher data transfer rates.

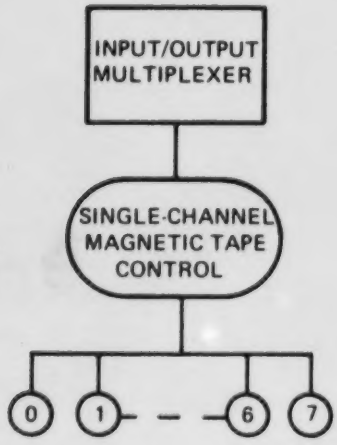


Figure 6-14.–Single-channel magnetic tape subsystem.

A single-channel magnetic tape subsystem connected to an IOM permits reading or writing of any one of up to eight magnetic tape units connected to that control (fig. 6-14). Reading or writing proceeds simultaneously with other peripheral operations on other peripheral channels and with processor operations.

Dual-channel control of a magnetic tape subsystem provides for atuomatic overlapping of read and write operations on any of the associated tape units. As shown in figure 6-15, a subsystem including a dual-channel control and two or more tape units permits accessing of any tape unit through either channel and tape control. Thus, if one channel is busy with an assigned tape unit, access can be gained to any other tape unit on the subsystem through the other channel.

As shown by the dotted line, a magnetic tape subsystem featuring dual-channel control can be connected between two IOMs.

URC001 and URC002 Unit Record Controls

Unit record controls connect multiple unit record devices to the Series 6000 central system. As many as seven devices can be controlled simultaneously by a unit record control, while requiring only a single interface to the Series 6000 central system (fig. 6-16).

Two versions are offered: the URC001, which is physically integrated into the input/output multiplexer (IOM); and the URC002, a freestanding control. Both versions have identical functional capabilities.

CONNECTED DEVICES.–The URC001 and URC002 unit record controls are completely

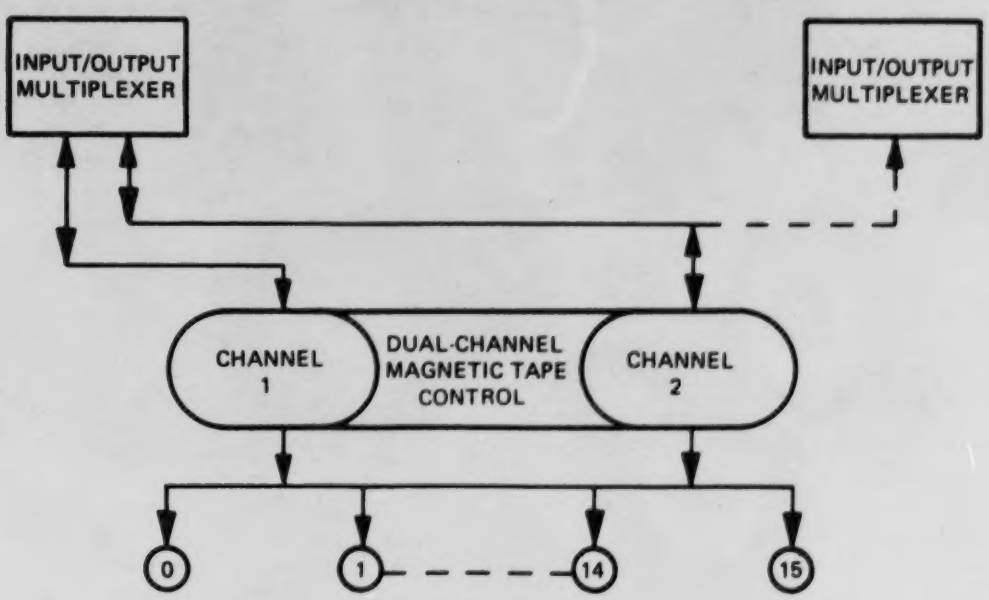


Figure 6-15.—Dual-channel magnetic tape subsystem.

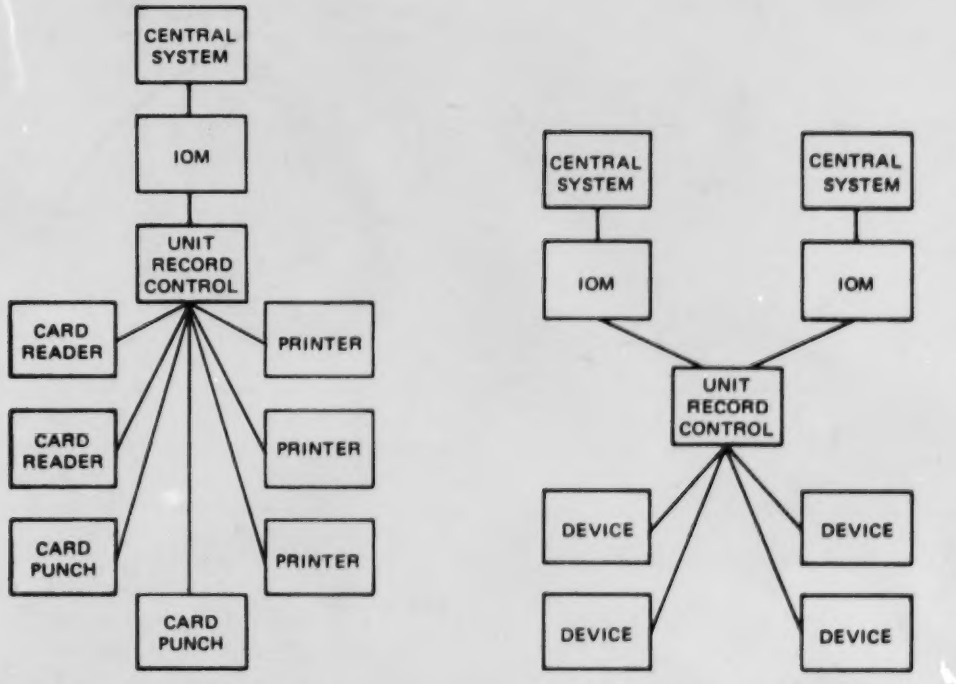


Figure 6-16.—URC001 and URC002 configurations.

flexible; either control can connect one to seven unit record devices, in mixed combinations. The following devices can be connected to the unit record control:

- Type CRZ301 card reader–1,050 cards per minute
- Type CPZ300 card punch–100 to 400 cards per minute
- Type PRT203 drum printer–1,100 lines per minute
- Type PRT303 train printer–1,150 lines per minute

MAXIMUM CAPACITY.–A unit record control controls a maximum configuration of two CRZ301 card readers, two CPZ300 card punches, and three PRT203 or PRT303 printers (or a combination of these printers) at their maximum rated device speeds. As many as seven devices can be multiplexed through a single channel to the input/output multiplexer.

MULTIPLE CHANNELS.–As many as three additional IOM channels (a total of four) are optionally available with either the URC001 or the URC002 unit record control. The addition of these channels permits the unit record subsystem to be shared by multiple central systems. When the subsystem is used by more than one system through multiple IOMs, individual devices must be dedicated to a specific central system.

PRT303 Printer

The PRT303 printer is a high-performance train printer equipped with interchangeable "train cartridges" that produce exceptional print quality, with excellent vertical and horizontal alignment (fig. 6-17). In addition, the PRT303 utilizes a power-driven hood and stacker, and noise-suppressant panels for greater efficiency and quieter operation.

The PRT303 can be connected either to the Type URC001 integrated unit record control in the input/output multiplexer, or to the freestanding URC002 unit record control. The data medium consists of continuous, fanfold forms up to 21 inches wide and 22 inches long. It prints the original and up to five copies and handles single-part, continuous, or tabulating card stock.

78.179

Figure 6-17.–PRT303 printer.

SPEEDS.–Rated speed for the PRT303 printer is 1150 lines per minute (1pm) nominal (48-character set). Speed is based on character set size, configuration, and utilization. The standard print trains for the PRT303 are the BCD set with 63 printable characters and the ASCII set (upper/lower case) with 94 printable characters. These standard character sets are preferred train sets which provide the best average print speeds.

TRAINS.–The train cartridges are interchangeable by the operator, and include the standard BCD print train cartridge, and the ASCII (upper/lower case) print train cartridge. Each train holds 288 character positions. Other train cartridges are available on special request.

CHARACTER SETS.–There is a choice of standard character sets of 63 (BCD mode) or 94 (ASCII mode) different printable characters per

train cartridge. Various special type fonts or characters are available on special request.

CHECKING.–The PRT303 illuminates warnings for: Paper low–Out of paper–Incorrect parity in paper loop–Hammer drive fuse failure–Paper feed error–Buffer overflow–Parity error on characters in printer line buffer–Parity on train image characters in buffer–Parity on address to printer.

PRINT MODES.–The edit print mode allows character-controlled skipping by using control characters in the data line. The nonedit print mode prints all 63 printable characters of the Series 6000 standard BCD character set.

In the ASCII mode, all 94 printable characters of the standard ASCII character set are printed. Features of PRT303 printer are:

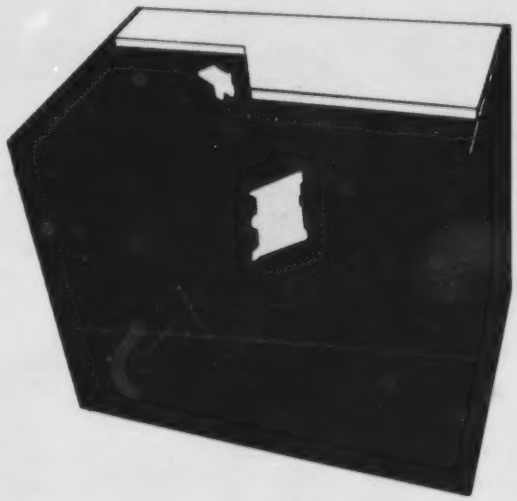
1. URC control of up to three printers.
2. Power hood and power stacker.
3. Noise suppression panel for quiet operation.
4. Paper skipping up to 70 inches per second, uses a 2-speed slew.
5. Vertical format is controlled by print command: single, double, top of page, or no spacing. Paper can be skipped to any of 15 coded positions on the paper tape loop: 0 to 15 lines by countdown, or skipped to the top of the page.
6. Horizontal format character can cause 8 to 120 (in multiples of 8) blank positions to occur in the print line.
7. Line width is 136 characters; 10 characters per inch.
8. Operator selects six or eight lines per inch.
9. Automatic standby turns off the print train, ribbon drive mechanism, and paper stacker automatically when not used for a specified period of time.
10. Two-level overtemperature sensing provides a warning indication prior to final shutdown in event of overtemperature.
11. Improved fault detection provides useful maintenance aids.

CRZ301 Card Reader

The CRZ301 card reader is a photoelectric card input device. Demand feeding of cards permits a card cycle to begin at any time following completion of the previous cycle (fig. 6-18). The CRZ301 can be connected to either the URC001 Integrated Unit Record Control in the input/output multiplexer, or to the freestanding URC002 Unit Record Control. The data media may be either 80- or 51-column, 12-row cards; the data transfer modes are Hollerith and binary codes; the reading method is photoelectric with column-by-column feeding; and the speed is 1,050 cards per minute.

Two checks, validity and cycle, are performed at the time of data transmission. The validity check is for an illegal punch. The cycle check is for failure of the photocell circuitry and/or timing signal generator. Failure of either check sets a program-accessible status indicator which can be used to effect a branch to a corrective routine.

The card reader responds to a failure of either check by offsetting the error card in the stacker. At the same time, a check indicator



78.180

Figure 6-18.–CRZ301 card reader.

light on the operator panel is also illuminated, calling attention to one or more device status indicator lights.

Features of the CRZ301 card reader include:

1. URC control of up to two card readers.
2. Read hopper capacity of 3,000 cards.
3. Stacker capacity is 2,500 cards.
4. Data Protection using validity check; cycle check; offset stacking of misread cards; read data comparison check–double read per column.
5. Reads intermixed Hollerith and binary cards.

CPZ300 Card Punch

The CPZ300 card punch is a high-speed card output device (fig. 6-19). Punching speed is variable as an inverse function of the amount of data to be punched in each card. Punching is provided in Hollerith or binary.

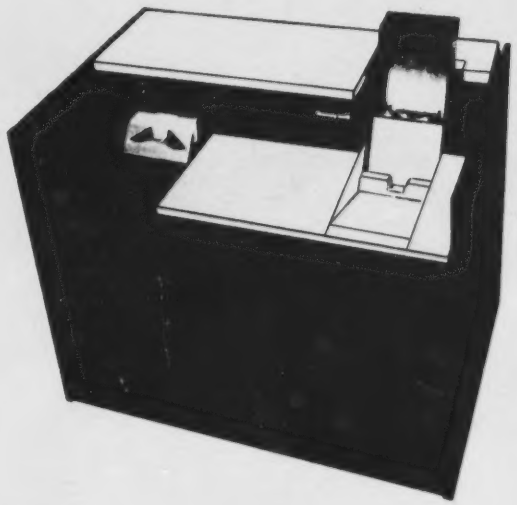
The CPZ300 can be connected either to the URC001 integrated unit record control in the input/output multiplexer, or to the freestanding URC002 unit record control. The data media consists of 80-column, 12-row cards and the data transfer modes are Hollerith and binary codes. The punching method is dual-column punching with column-by-column feeding.

The speed varies from 200 to 400 cards per minute, depending upon the exact number of blank column pairs and their location on the card.

Data protection is accomplished through punching error detection. Punching errors are detected by sensing the punches that have been activated and automatically comparing the result with the data specified for punching.

Features of the CPZ300 card punch include:

1. URC control of up to two card punches.
2. Hopper/stacker capacity of 1,600 cards each.
3. Nonstop card loading and unloading while processing.
4. Data protection using punch activation check and punch parity check. Mispunched cards are offset stacked.
5. High-speed skip provides a significant increase in punching throughput on applications employing a gap between fields.



78.181

Figure 6-19.–CPZ300 card punch.

CHAPTER 7

DOCUMENTATION PREPARATION AND STANDARDS

According to the Dictionary for Information Processing (FIPS PUB 11-1), the definition of documentation is "The management of documents which may include the actions of identifying, acquiring, processing, storing, and disseminating them. A collection of documents on a given subject." A document is a medium and the data recorded on it is for human use. By extension, a document is any record that has permanence and can be read by human or machine. With the foregoing in mind, it is easy to see the important relationship documentation has with the data processing world.

The first part of this chapter will discuss, in general, the requirements prescribed for documentation preparation standards in SECNAVINST 5233.1 series, entitled Department of the Navy Automated Data Systems Documentation Standards. The discussion, although skeletal in form, is complete enough to acquaint the DP2, DP1, or DPC with the document components that are required for a production-ready documentation package. The last part of the chapter will discuss explicit details of actual documentation standards as required by the Department of Defense Instruction 7935.1 (series), entitled DOD Automated Data Systems Documentation Standards. Not every type of document can be discussed in this rate training manual because of space limitations. Only the most commonly used manuals, such as the Computer Operation Manual, will be discussed.

NEED FOR STANDARD DOCUMENTATION

You are on your way to becoming a First Class or Chief Petty Officer, and now you will be the one to answer questions rather than ask them. Your quest for knowledge will now, more than ever, be directed into the written documentation that surrounds, and sometimes seems to smother those in supervisory and management positions.

If the material with which you are dealing is too wordy or confusing in format, time is lost and the material is not fully utilized. The documentation standards adopted in SECNAVINST 5233.1 series have done much to help management avoid this waste.

When automatic data processing was adopted into everyday use in the Navy, a sudden and realistic need for documented procedures presented itself to management.

The passing of information from person to person, as the need arose, quickly became obsolete, and a method of factual, detailed, and concise documentation was developed. The guidelines for this method, discussed later in this chapter, are contained in SECNAVINST 5233.1 series.

Many articles have been written concerning the need for Automated Data System (ADS) documentation and its standardization. Following are just a few of the purposes that documentation serves.

1. It provides managers with documents to review at significant developmental milestones to determine if requirements have been met and if resources should continue to be expended.

2. It records technical information to allow coordination of later development and use/modification of the ADS.

3. It ensures that authors of documents and managers of project development have a guide to

follow in preparing and checking documentation.

4. It provides uniformity in the format and content of computer programs, documentation, and ADS, across command lines.

SECNAVINST 5233.1 series has provided standards for recording information required for computer programs to ensure that the documentation produced will serve the aforementioned purposes. These standards apply to the following types of computer programming documents:

DOCUMENT TYPE NAME/MNEMONIC IDENTIFIER

1. Functional Descriptions (FD)

2. Data Requirements Documents (RD)

3. System/Subsystem Specifications (SS)

4. Program Specifications (PS)

5. Data Base Specifications (DS)

6. Project Manuals (PM)

NOTE: Project manual mnemonic assignment occurs only for small projects when the Users, Computer Operations, and Program Maintenance manuals are bound as a single document of under 200 pages. After the combining of these manuals is complete, they are designated as a Project Manual (PM).

7. Users Manuals (UM)

NOTE: Under certain circumstances, the commanding officer may authorize minimum documentation requirements in a Users Manual. These circumstances include (1) when computer programs have been developed exclusively for internal use at the local level, (2) when programs will be used on a one-time basis or for no longer than 3 months duration, and (3) when programs have no identifiable use elsewhere in the government. An annotated program listing should be included in the Users Manual.

8. Computer Operation Manuals (OM)

9. Program Maintenance Manuals (MM)

10. Test Plans (PT)

11. Test Analysis Reports (RT)

12. Implementation Procedures (IP)

Other documents that are to be prepared in accordance with these standards, when applicable, include Technical Reports (TR) and Technical Notes (TN). A Technical Report (TR) is a document that reports the results of a completed project, basic research, or developmental study. A Technical Note is a document that provides procedures, lists of data, or other information that does not logically belong in other types of documents.

DOCUMENT COMPONENTS

Each of the 11 types of documents in the preceding list is a complete work within itself. That is, each type is a complete manual or report which explains or supports the title of the document. (The PM (Project Manual) is not counted as a single type of document because it encompasses three manuals.) The OM (Computer Operation Manual), for example contains precise and detailed information on the control requirements and operating procedures necessary to successfully initiate, run, and terminate the subject system. This documenting is done by supplying the relevant information called for by the standard outline in SECNAVINST 5233.1 series and DOD Instruction 7935.1 series. Once the information is supplied to completely fulfill the requirements for an OM, it is then put into manual form as a self-standing document.

Within the covers of each of the 11 types of documentation are optional and required components. Each document is structured from

the following components, in the sequence listed:

1. Front cover	(Mandatory)
2. Title page	(Mandatory)
3. Special notices	(As required)
4. Abstract	(Mandatory in FD, UM, PM, and TR)
5. Table of contents	(Mandatory)
6. List of figures	(As required)
7. Record of changes	(As required)
8. List of effective pages	(Mandatory in classified documents)
9. Text	(Mandatory)
10. Appendixes	(As required)
(a) Terms and abbreviations	(As required)
(b) References	(As required)
(c) Bibliography	(As required)
(d) Other appendixes	(As required)
11. Index	(Optional)
12. Distribution list	(Mandatory)
13. Back cover	(Mandatory)

In the following sections, a brief description, including an example and format layout of each mandatory and optional component of a document, is discussed. When actually documenting an ADS, SECNAVINST 5233.1 series should be referenced.

Front Cover

A front cover for each document is mandatory and contains the information shown in the format layout in figure 7-1 and in the example in figure 7-2:

1. The document title and subtitle (may include a superseding statement).
2. The activity short name.
3. The document number. The document number consists of the project number under which the document is produced, followed by a control number to identify the individual document. On both the cover and title page, the document number appearing beneath the designator of the preparing organization is formatted in the following manner:

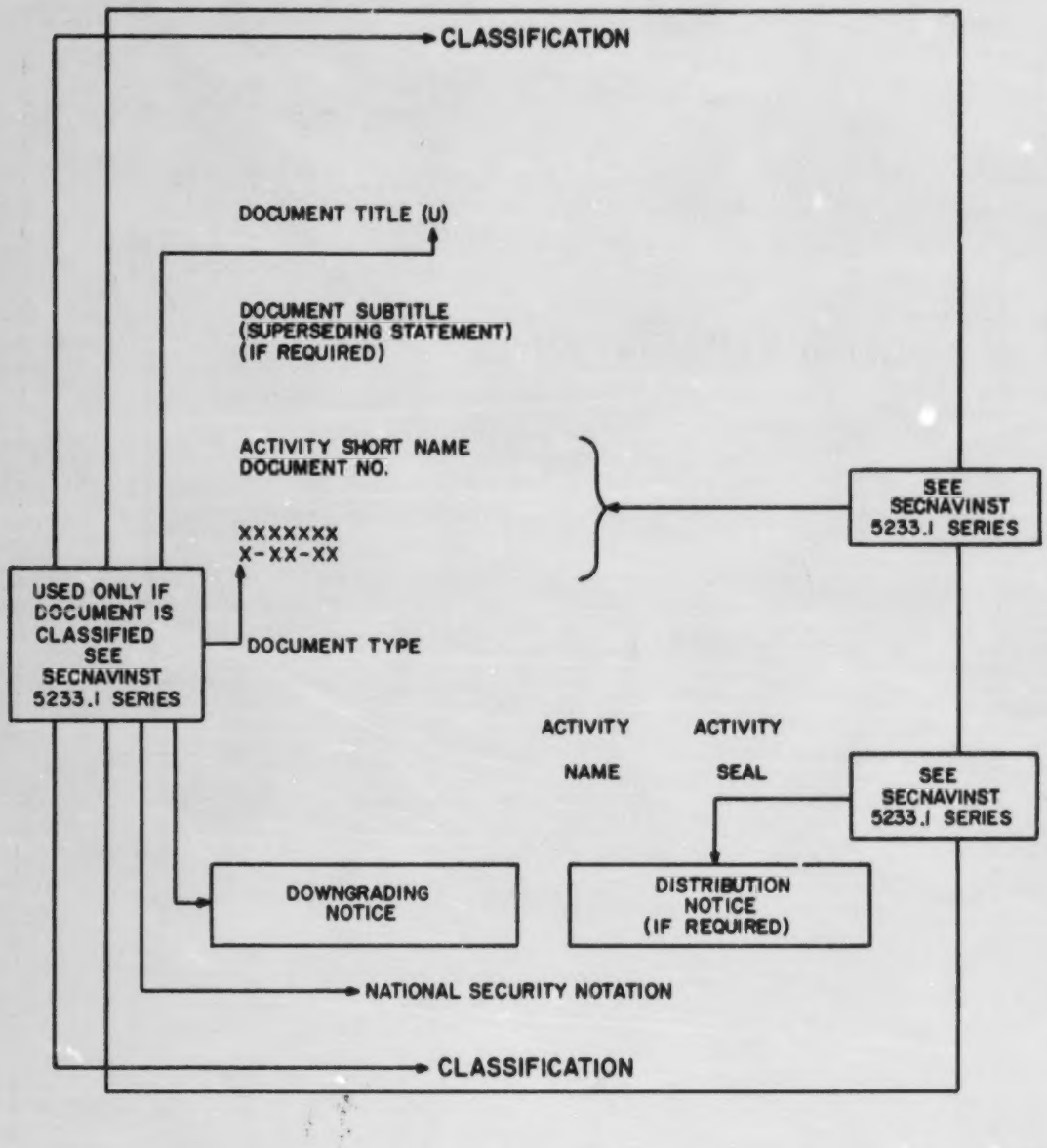
NARDACWASHDC DOCUMENT NO.

(project no.)	98T1003
(control no.)	C-PS-04A

The alphanumeric project number uniquely identifies the project effort and also may be used for budgeting and funding control. The first and second characters of the project number indicate the requesting organization; the third character specifies the function of the project; the fourth character identifies the organization responsible for development of the project; and the fifth, sixth, and seventh characters form a serial number for the given requestor, functional area, and organization responsible for development.

4. The type of document. The first character of the control number is the classification of the document. The characters used are "T" for TOP SECRET, "S" for SECRET, and "C" for CONFIDENTIAL. If the document is unclassified, no letter designator is used. The second and third characters are the mnemonic identifiers for the document type and are preceded and followed by a dash ("-"). The fourth and fifth characters are the document type count. The document type count consists of two digits assigned from a consecutive count of the same type of documents generated on the project. The first document of a particular type is numbered "01." For any project with over 99 documents of one type, a third digit may be added, starting with the numeral "100." The sixth character, which follows the document type count, is alphabetic and is used to identify a document which has been revised. A new, consecutive character is used for each reissue or major change, starting with "A" for the first revision. When a revision letter is used, the document preceding the revision is normally cancelled.

The preceding example (fig. 7-2) refers to a confidential Program Specification (PS)



78.155

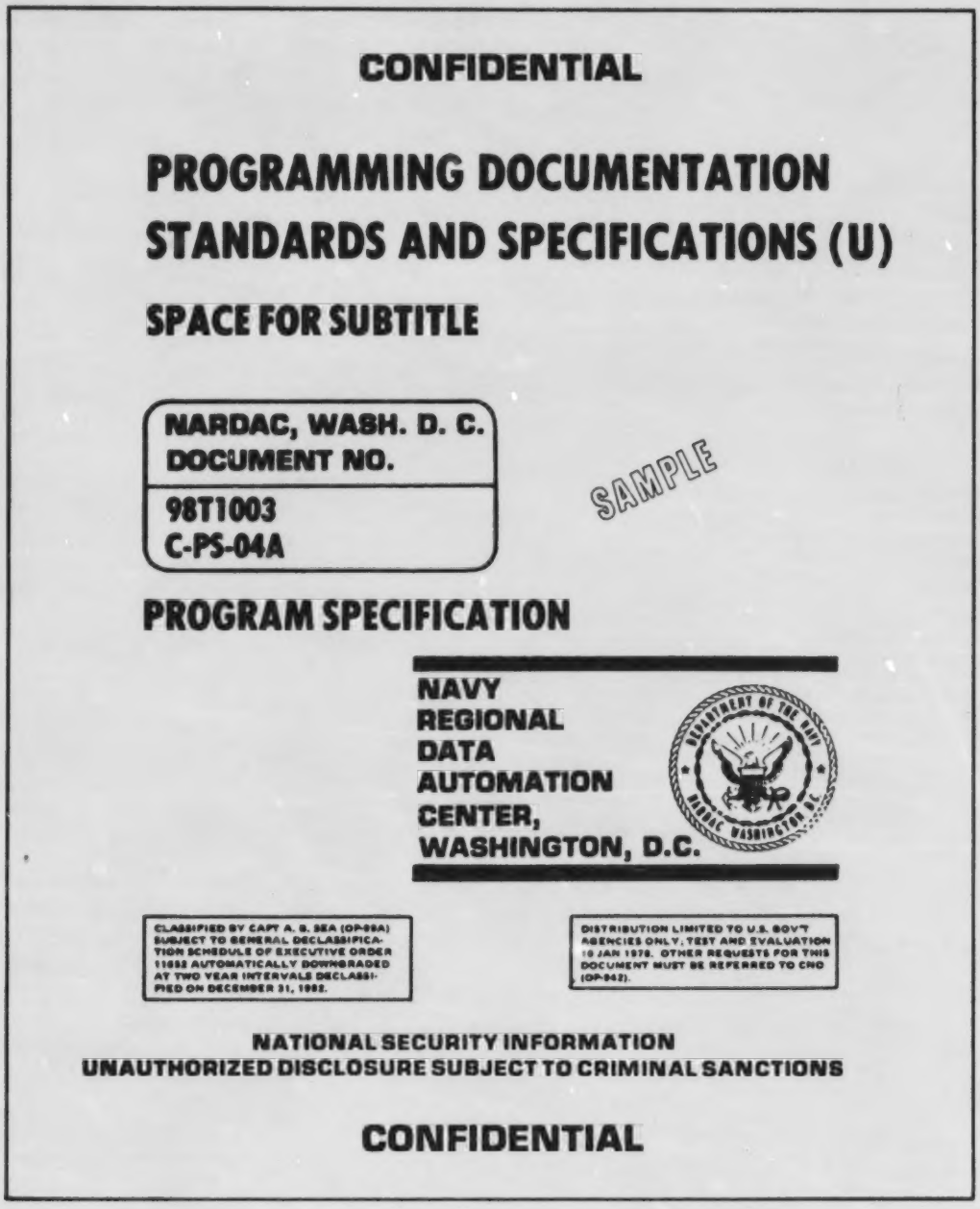
Figure 7-1.—Layout of front cover.

prepared by NARDACWASHDC for project 98T1003. The document is the fourth Program Specification (PS) in the series and has been revised once since the original document was prepared.

5. The activity name.

6. The activity seal.

7. The security identification (includes classification of the document, downgrading notice, distribution notice, and national security notation if classified.) See SECNAVINST 5233.1 series.


CONFIDENTIAL
PROGRAMMING DOCUMENTATION STANDARDS AND SPECIFICATIONS (U)
SPACE FOR SUBTITLE
NARDAC, WASH. D. C.
DOCUMENT NO.
98T1003
C-PS-04A
SAMPLE
PROGRAM SPECIFICATION
NAVY
REGIONAL
DATA
AUTOMATION
CENTER,
WASHINGTON, D.C.
CLASSIFIED BY CAPT A. B. SEA (OP-95A) SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS DECLASSIFIED ON DECEMBER 31, 1982.
DISTRIBUTION LIMITED TO U.S. GOV'T AGENCIES ONLY; TEST AND EVALUATION 10 JAN 1978. OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO CNO (OP-942).
NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE SUBJECT TO CRIMINAL SANCTIONS
CONFIDENTIAL

78.156

Figure 7-2.–Example of front cover.

Title Page

The title page of each document is mandatory and has the information shown in the format layout in figure 7-3 and the example in figure 7-4.

1. The activity name.

2. The document title and subtitle.

3. The type of document.

4. The date.

5. The activity short name.

6. The document number (same format as on the front cover).

7. The user designator, if the document is prepared for a specific user.

8. The contractor and contract number designation, if the document has been prepared by a contractor under the guidance of the approving activity.

9. The security identification. (See SECNAVINST 5233.1 series.)

10. The copy number.

The actual layout of the preceding items may vary when circumstances require the use of a "window" front cover, which displays a portion of the title page as part of the front cover.

Special Notices

Special notices in each document are on an "as required" basis. An "as required" basis is simply an item that is required by document content or higher authority instructions or special interest, for example, special security handling procedures. Special notices may contain information concerning the status of a document, instructions for its handling, letters of promulgation, the status of the contents of the document, the date the provisions of the document become effective, credit to an individual or organization for the preparation of the document, or such other information as may be pertinent. The titles of such special notice pages generally reflect the subject matter of the information provided.

Abstract

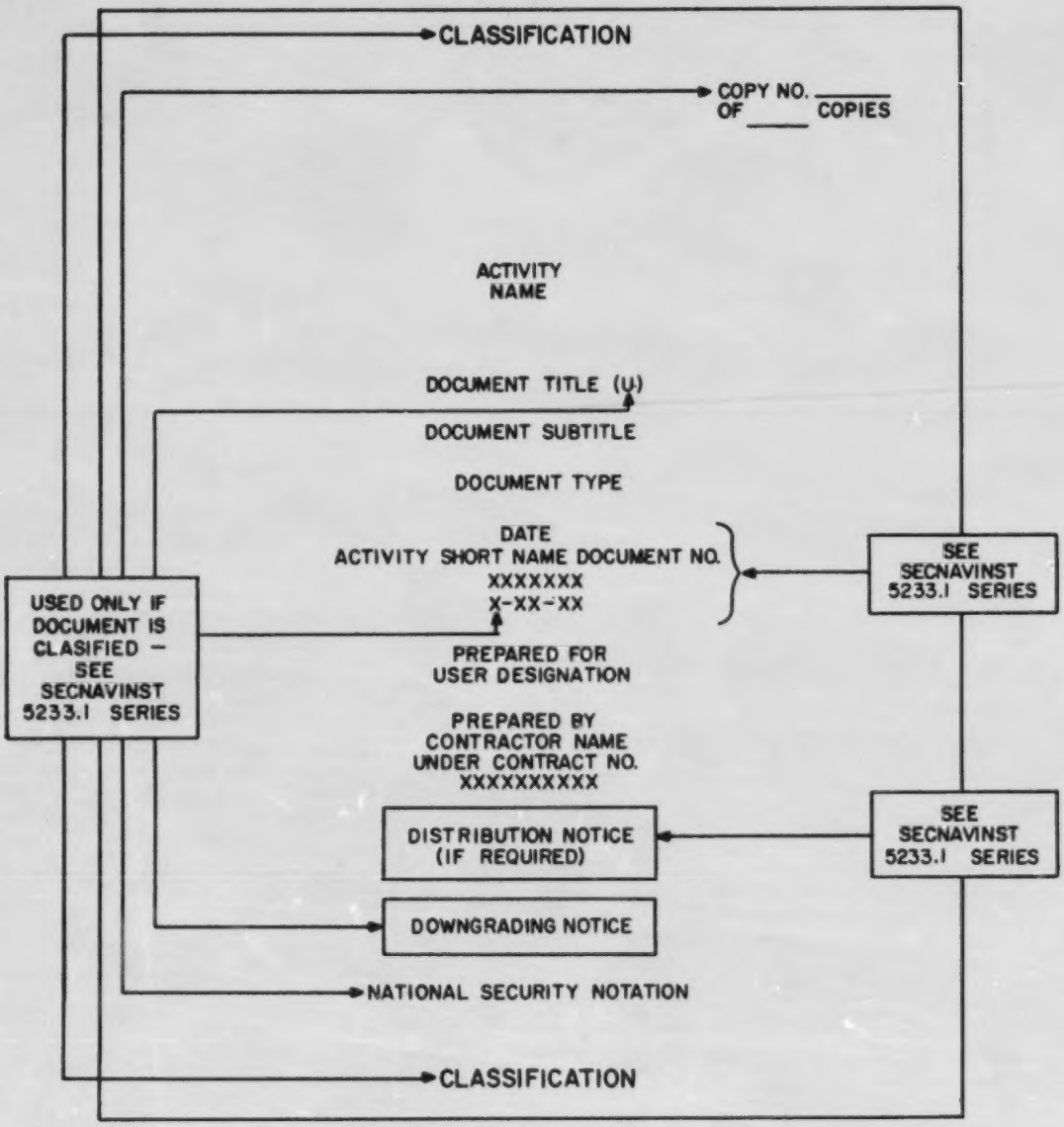
An abstract is mandatory in FD, UM, PM, and TR documents. The abstract is a brief summary (not to exceed 250 words and preferably unclassified) of the function, purpose, scope, and content of the computer program/system or study described in the document. Information concerning inputs, processing, and outputs must be included in the abstract of computer programs/systems. An abstract of a study must summarize essential facts, findings, conclusions, and recommendations. The purpose of the abstract is to assist potential users in determining the usefulness of certain subject matter to their particular environment and to summarize the most significant material in the document clearly and concisely. The abstract should be in narrative form and include no special characters.

Table of Contents

The table of contents is mandatory for each document and lists the identification number or code, the title, and the page number of each section. The numbered paragraphs in the text, as well as each appendix and the numbered paragraphs in each appendix (if applicable), are also listed. Tabulation is ordinarily at least to the third organizational level, e.g., 3.11.1.

List of Figures

The list of figures is on an "as required" basis and accounts for each figure included in the text and appendixes of a document. The figure number, its title, and a beginning page number are shown for each figure.

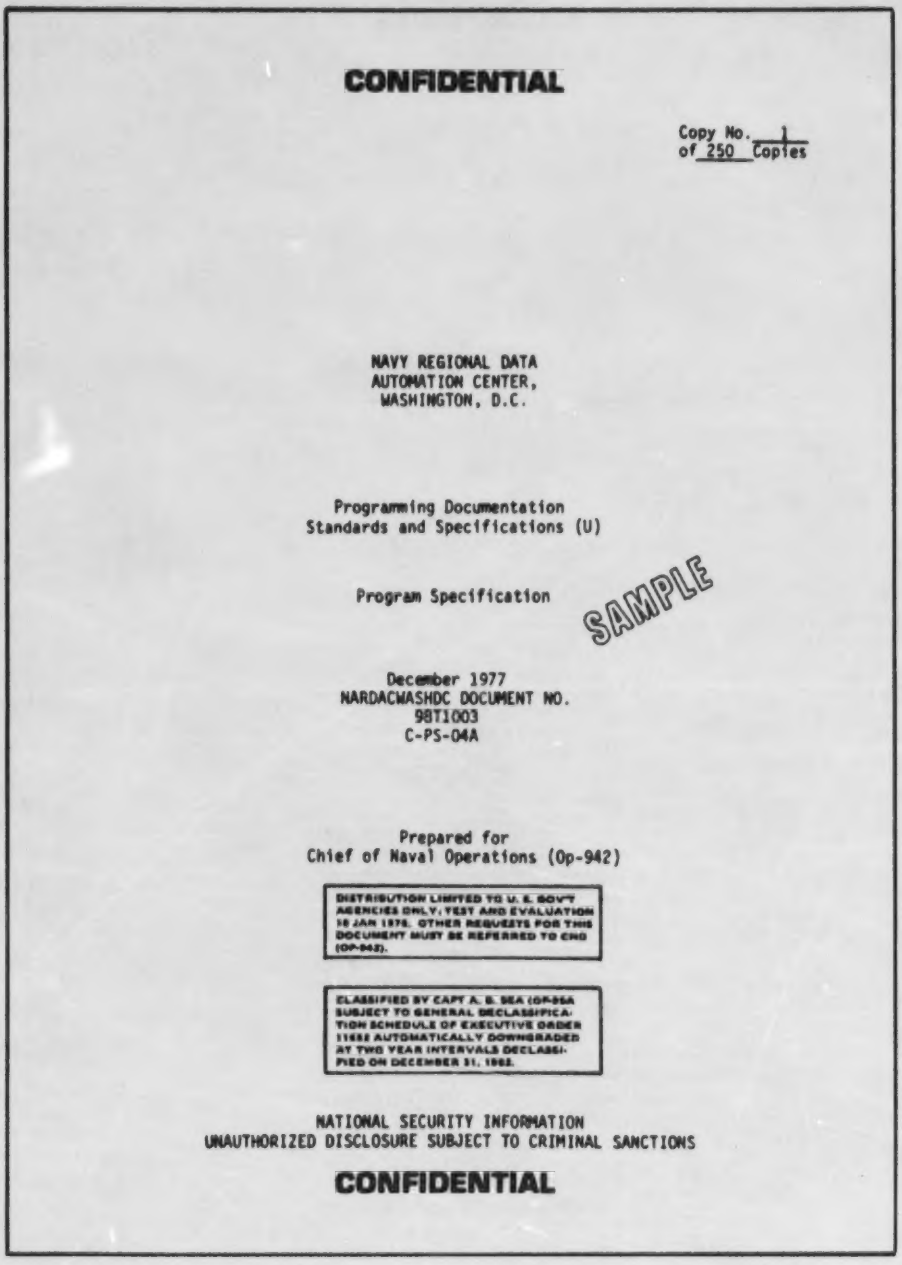


78.157

Figure 7-3.–Layout of title page.

Record of Changes

The record of changes page is used on an "as required" basis and should be inserted in a document starting with the first change. The record of changes page is used to record changes made to a document, and is included at origination, when frequent changes to the document are expected. This page is arranged in columnar form and provides spaces for the change number, the date of the change, the date the change is entered, and the signature of the



CONFIDENTIAL

Copy No. 1
of 250 Copies

NAVY REGIONAL DATA
AUTOMATION CENTER,
WASHINGTON, D.C.

Programming Documentation
Standards and Specifications (U)

Program Specification

SAMPLE

December 1977
NARDACWASHDC DOCUMENT NO.
98T1003
C-PS-04A

Prepared for
Chief of Naval Operations (Op-942)

DISTRIBUTION LIMITED TO U. S. GOV'T AGENCIES ONLY; TEST AND EVALUATION 16 JAN 1978. OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO CNO (OP-942).

CLASSIFIED BY CAPT A. B. SEA (OP-05A SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS DECLASSIFIED ON DECEMBER 31, 1982.

NATIONAL SECURITY INFORMATION
UNAUTHORIZED DISCLOSURE SUBJECT TO CRIMINAL SANCTIONS

CONFIDENTIAL

78.158

Figure 7-4.—Example of title page.

individual making the change. The record of changes page follows the format layout shown in figure 7-5.

A change transmittal notice should be issued by the authority responsible for the maintenance of the document being changed. It should include a reference to the document, a list of the actions to be taken to complete the change, a cancellation notice, if appropriate, and any other information or directions necessary to keep the document current and properly effect the change.

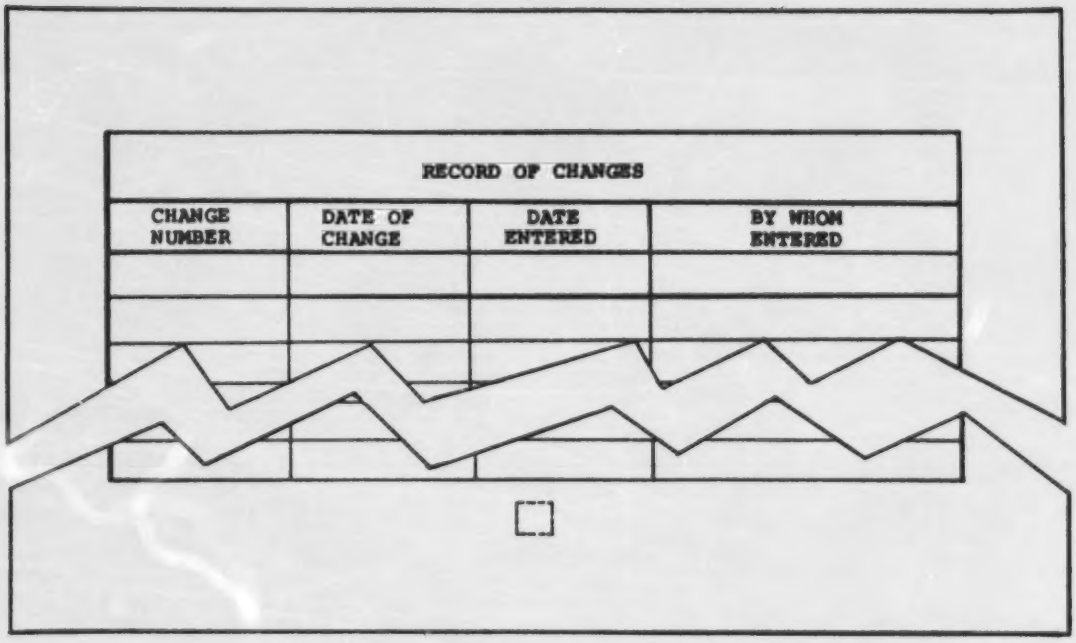
The revised text of the document should be either attached to the change transmittal notice as the page(s) to be inserted into the document or specified by a list of pen changes in the body of the notice. (See fig. 7-6.)

Page changes are preferable to pen changes, since they are generally more economical, provide a neater product, decrease the chance of errors, and decrease the time expended by the ADP staff in making changes.

A list of changes to be made by deleting, changing, or adding information by pen should be provided when the time required to enter all of the changes does not exceed the time required to replace the sheet. Directions must state precisely where the change occurs and include the page number, paragraph number, line number, and other pertinent information necessary to make the change correctly.

List of Effective Pages

A list of effective pages is mandatory in classified documents and optional in unclassified documents. This list should be provided when frequent changes to a document are expected or when strict page accountability is desired. Each page of the document and its change number



78.159

Figure 7-5.—Layout of record of changes page.

NAVY REGIONAL DATA AUTOMATION CENTER, WASHINGTON
WASHINGTON NAVY YARD
WASHINGTON, D. C. 20374

IN REPLY REFER TO
Code 70
Ser

NARDACWASHDC DOCUMENT NUMBER 98T1003 TN-01 CHANGE TRANSMITTAL 1

From: Commanding Officer, Navy Regional Data Automation Center, Washington, D.C.

Subj: Documentation Standards

Encl: (1) Revised pages 1, 2, and 3

1. Purpose. To transmit Change 1 to the subject document.

2. Action

a. Pen change. In paragraph 2.2, item d, delete "(Optional)" and insert "(Mandatory)".

b. Page changes. Remove pages 1, 2, and 3 and insert enclosure (1).

s/Commanding Officer

Distribution:
(see next page)

78.160

Figure 7-6.—Example of change transmittal notice.

should be listed. An example is shown in figure 7-7.

When a list of effective pages is required in a document, it must be updated with each change transmittal notice that adds pages to or replaces pages in the document. The revised list should be forwarded with each change transmittal notice unless only pen changes are to be made to the document.

Text

The text of each document should conform to the prescribed content as set forth in SECNAVINST 5233.1 series. Figures may be used in the text to clarify or illustrate the technical content. The instructions, content requirements, and format for a Project Manual (PM) which contains the Users Manual (UM), the Computer Operation Manual (OM) and the Program Maintenance Manual (MM) are attached to this rate training manual as appendix II. This appendix should be reviewed thoroughly prior to taking advancement in rate examinations.

Appendixes

Appendixes are used on an "as required" basis. They should contain material which supports, but is not readily incorporated into, the text of a document. Included within the appendixes may be narrative material or illustrations which should generally be sequentially referenced in the text and listed in the same order in the table of contents. When appendixes are classified or bulky, they may be bound separately. The following three basic appendixes should be provided.

Terms and Abbreviations.–This appendix provides definitions of acronyms and abbreviations used within the document. Any terms or phrases appearing in dictionaries or accepted data processing vocabularies, such as NAVSO P-3097 and FIPS PUB 11-1, need not be defined.

Explanations of terms unique to specific computer programs may be provided, but should be separated from the terms and abbreviations appendix. Item names, location tags, and short program names may be included, and a cross-reference to the full name of the computer program that uses these tags and names should be provided.

References.–This appendix is provided if more than 10 sources are cited in the text. All references listed must be referred to in the text and should be presented in the same general order as they are referenced in the text. Each source listed in the appendix must be identified by an Arabic numeral. The identifying information for each reference is presented in the following order: (a) Books–Author's name, name of the book, book identification number, place of publication, name of the publisher, date of edition, and pages being cited. (b) Periodicals–Author's name, title of the article, name of the periodical, volume number, date, and pages being cited.

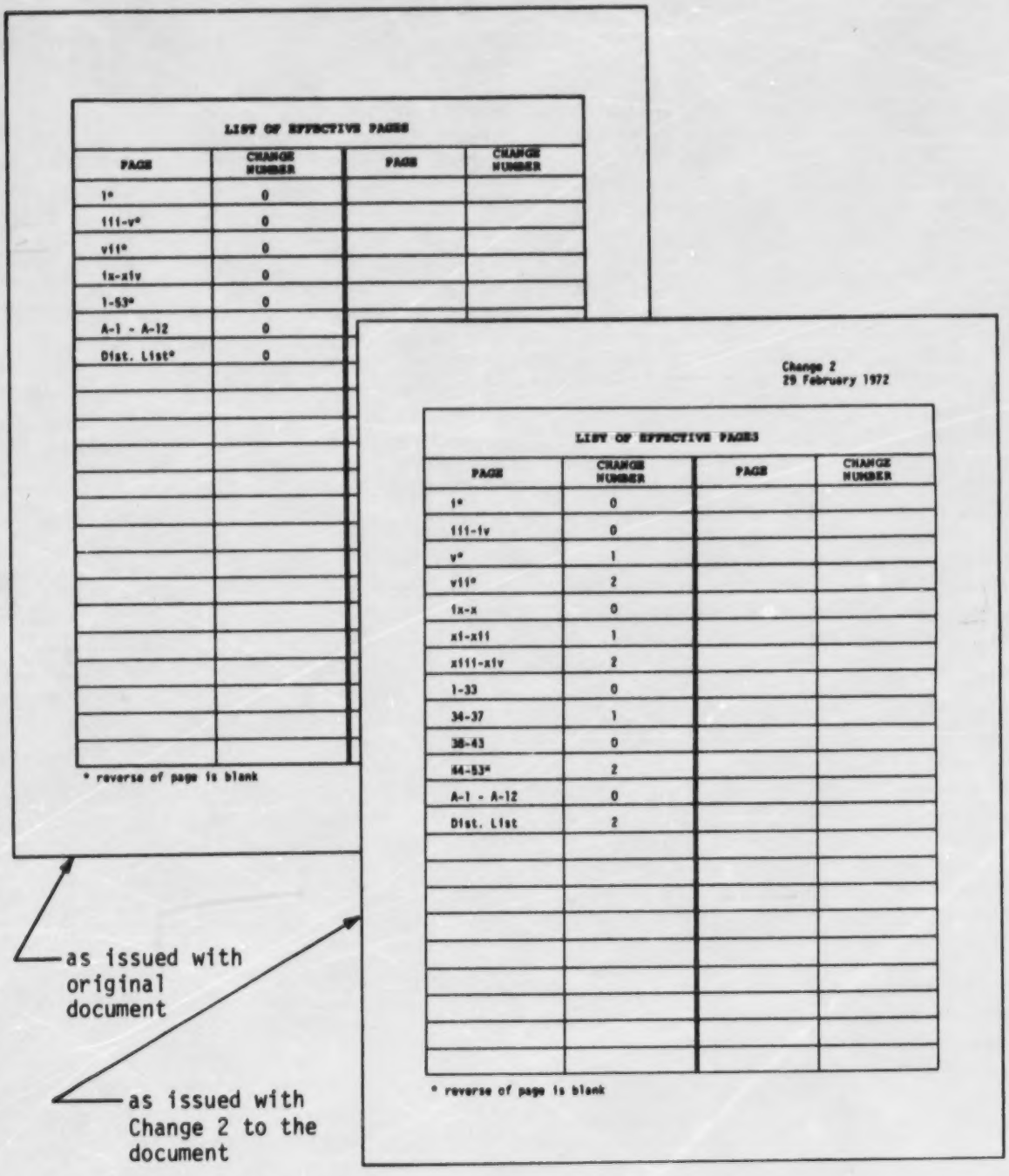
Bibliography.–This appendix provides a list of indirect references which are worthy of note by the reader. A source listed in the bibliography needs no identifying number, but must be listed in alphabetical order according to last name of the author. References not credited to a specific author should be listed first. A short summary, not to exceed four lines, may be provided for each bibliography listing.

Index

An index is an optional component and should contain an alphabetical list of names, subjects, and the like, together with the paragraph number of each.

Distribution List

The distribution list is a mandatory component and is composed of the names and codes of commands, activities, and offices, external to the originating organization, which receive copies of the document. When wide distribution is planned, the Standard Navy Distribution List (SNDL) codes should be used.



78.161

Figure 7-7.—Layout of lists of effective pages.

Back Cover

The back cover is a mandatory component and is blank, except for the security classification if the document is classified.

DOCUMENT DOCUMENTATION REQUIREMENTS

In the first part of this chapter documentation components were discussed. In the second half, the documents themselves will be discussed including a summary of the purpose of each document. The required contents of the Computer Operation Manual, Users Manual, and Program Maintenance Manual are thoroughly discussed in the appendixes. Every type of document may not be needed on every project. The project manager must determine early in the development process which of the types of document will be needed for the project.

One of the main determining factors for the number of documents to be provided is the ultimate user. If the user is not computer oriented, it may be beneficial to the project manager and the user to provide all the documentation. This will allow for explanation of as much of the system (hardware and software) as possible in a language that the user can understand. The more the user understands about the actual functioning of the system, the better for both parties. Once understanding is developed, communication becomes easier, not only in the area of the current project but also for any future dealings.

If the project is large and complex, the maximum amount of documentation should be provided. Under these circumstances it does not matter if the user is or is not computer oriented. The better and more complete the documentation is in this case, the better the final product (system) will be. The more documentation produced, the less likely it will be that any portion of the system will be left out.

To further help in determining the need for proper documentation, refer to the chart in figure 7-8. This chart lists complexity factors, with five values assigned to each factor. The more complex, costly, or time restricted a factor is, the more value it holds. To utilize the chart for a project, simply put a check mark beside the descriptive block that is most accurate for each factor. Total the check marks for each column and multiply that times the value for that column. For instance, there may be a total number of four check marks in column one and a total value for that column of four (4 times 1 equals 4); four check marks in column two for a total value of eight (4 times 2 equals 8); three check marks in column 3 for a total value of nine (3 times 3 equals 9); and no check marks in columns four or five. Each column's value totals are then added together for one total (in this case 21), which is the level of project complexity.

Once a level of project complexity has been established, the types of documentation needed can then be determined. Figure 7-9 is suggested as a method of determining the documentation requirements based on the complexity totals. In the preceding example, the complexity total of 21 would require the writing of a Users Manual, a Computer Operations Manual, a Program Maintenance Manual, and a Test Plan.

It must be emphasized that this is a general guide. Situations occur when more or fewer types of document may be required, as is indicated in the notes of figure 7-9.

The Navy has established documentation standards to ensure completeness and uniformity for computer system information between commands and between civilian and Navy organizations. The amount of detail and the time/cost factor of such program documentation for "in-house" use at the local level may be too great. In these instances, options are given to the commander/ commanding officer providing the resources and/or funds to establish appropriate minimum documentation requirements less than those established in SECNAVINST 5233.1 series.

Local minimum documentation requirements are usually established by the head

COMPLEXITY: / FACTORS	1	2	3	4	5
1. ORIGINALITY REQUIRED	NONE, REPROGRAM ON DIFFERENT EQUIPMENT	MINIMUM, MORE STRINGENT REQUIREMENTS	LIMITED, MORE ENVIRONMENT, NEW INTERFACES	CONSIDERABLE, APPLY EXISTING STATE OF ART TO ENVIRONMENT	EXTENSIVE, REQUIRES ADVANCE IN STATE OF THE ART
2. DEGREE OF GENERALITY	HIGHLY RESTRICTED, SINGLE PURPOSE.	RESTRICTED, PARAMETERIZED FOR A RANGE OF CAPACITIES	LIMITED FLEXIBILITY; ALLOWS SOME CHANGE IN FORMAT	MULTI-PURPOSE, FLEXIBLE FORMAT, RANGE OF SUBJECTS.	VERY FLEXIBLE, ABLE TO HANDLE A BROAD RANGE OF SUBJECT MATTER ON DIFFERENT EQUIPMENT
3. SPAN OF OPERATION	LOCAL OR UTILITY	COMPONENT COMMAND	SINGLE COMMAND	MULTI-COMMAND	DEFENSE DEPARTMENT, WORLD-WIDE
4. CHANGE IN SCOPE AND OBJECTIVE	NONE	INFREQUENT	OCCASIONAL	FREQUENT	CONTINUOUS
5. EQUIPMENT COMPLEXITY	SINGLE MACHINE ROUTINE PROCESSING	SINGLE MACHINE, ROUTINE PROCESSING, EXTENDED PERIPHERAL SYSTEM	MULTI-COMPUTER, STANDARD PERIPHERAL SYSTEM	MULTI-COMPUTER, ADVANCED PROGRAMMING, COMPLEX PERIPHERAL SYSTEM	MASTER CONTROL SYSTEM, MULTI-COMPUTER, AUTO INPUT-OUTPUT AND DISPLAY EQUIPMENT
6. PERSONNEL ASSIGNED	1-2	3-5	5-10	10-15	15 AND OVER
7. DEVELOPMENTAL COST	1-10 K	10-50 K	50-200 K	200-500 K	OVER 500 K
8. CRITICALITY	DATA PROCESSING	ROUTINE OPERATIONS	PERSONNEL SAFETY	UNIT SURVIVAL	NATIONAL DEFENSE
9. AVERAGE RESPONSE TIME TO PROGRAM CHANGES	2 OR MORE WEEKS	1 - 2 WEEKS	3 - 7 DAYS	1 - 3 DAYS	1 - 24 HOURS
10. AVERAGE RESPONSE TIME TO DATA INPUTS	2 OR MORE WEEKS	1 - 2 WEEKS	1 - 7 DAYS	1 - 24 HOURS	0 - 60 MINUTES
11. PROGRAMMING LANGUAGES	HIGH LEVEL LANGUAGE	HIGH LEVEL AND LIMITED ASSEMBLY LANGUAGE	HIGH LEVEL AND EXTENSIVE ASSEMBLY LANGUAGE	ASSEMBLY LANGUAGE	MACHINE LANGUAGE
12. CONCURRENT SOFTWARE DEVELOPMENT	NONE	LIMITED	MODERATE	EXTENSIVE	EXHAUSTIVE
TOTALS	X1=	X 2=	X 3=	X 4=	X 5=
					* COMPLEXITY TOTAL:

7-14

78.162

Figure 7-8.—Level of project complexity.

COMPLEXITY TOTAL	DOCUMENT TYPES			
12 – 15			UM OM MM	
12 – 26			UM OM MM	PT
24 – 38	FD		UM OM MM	PT
36 – 50	FD	SS	UM OM MM	PT RT
48 – 60	FD	SS PS	UM OM MM	PT RT

NOTES
1. PREPARATION OF THE DATA REQUIREMENTS DOCUMENT THE DATA BASE SPECIFICATION, AND THE IMPLEMENTATION PROCEDURES IS SITUATIONALLY DEPENDENT.
2. ADDITIONAL DOCUMENT TYPES MAY BE REQUIRED AT LOWER COMPLEXITY.

ABBREVIATIONS:

FD - FUNCTIONAL DESCRIPTION	OM - COMPUTER OPERATION MANUAL
SS - SYSTEM/SUBSYSTEM SPECIFICATION	MM - PROGRAM MAINTENANCE MANUAL
PS - PROGRAM SPECIFICATION	PT - TEST PLAN
UM - USERS MANUAL	RT - TEST ANALYSIS REPORT

78.163

Figure 7-9.–Types of documents/project complexity.

of the data processing department/division. At most commands this function is delegated to the project manager. These requirements are generally based on experiences of personnel who have been involved in writing, maintaining, and analyzing programs/systems, and in training new personnel to take the jobs of transferred personnel.

The key to the minimum amount of documentation required by local commands should be the amount that is required for replacement personnel to understand input, processing, and output for each program system for which they will be responsible.

TYPES OF DOCUMENTS

The following paragraphs provide a narrative discussion of the types of documents that may be produced during the evolutionary development of a computer program or system. It must be emphasized that the need for any one of these documents must be determined by the nature of the project, using the guidance provided in SECNAVINST 5233.1 series.

Functional Description (FD)

An FD (Functional Description) is normally prepared for any system requiring a basis for mutual understanding between the Development Group and the User Group of a proposed ADS. It reflects the definition of the system requirements and provides the ultimate users with a clear statement of the operational capability to be developed. If the scope of the FD is changed at any point during project development, the FD should be updated and receive user concurrence.

The FD is a tool for use by both computer- and noncomputer-oriented personnel and should be written, as much as possible, in noncomputer-oriented language, since many elements of the document will be subject to

review by staff personnel who do not necessarily have a computer background.

Data Requirement Document (RD)

The RD (Data Requirement Document) normally is prepared when a data collection effort by the User Group is required to generate and maintain system files. The RD is a technical document prepared by both development and user personnel. It should be as detailed as possible concerning the definition of inputs required of the user; the procedures to be followed to provide this input to the system; the description of expected output data; the specification of all uses of standard data elements; and the data limitations of the system.

The term "data element," as used throughout the RD, includes its related features. The term refers to a data element or to its use in a data system, often called the "data use identifier." The names and associated codes of many data elements have been standardized in order to facilitate data exchange and achieve commonality in data structures. These standard data elements and data element codes should be used whenever applicable in all data base files.

Automated data element libraries have been developed and are being used by various organizations within the Department of Defense. These data element libraries identify and define the data elements used by a particular organization, reference the systems and files in which they are used, and associate these data elements to applicable data elements and data code standards. When a data processing system is designed that uses standard data elements or uses data elements that have not yet been standardized, any existing data element libraries should be updated to reflect the new uses.

System/Subsystem Specification (SS)

An SS (System Specification or Subsystem Specification) may be prepared to guide the development of large projects. If the system breaks down readily into subsystems, this document may be used to prepare individual Subsystem Specifications. A subsystem is herein defined as the logical breakdown of a system into separate areas of responsibility, such as functions, where each breakdown is composed of a program or a series of programs. If individual Subsystem Specifications are prepared, they may at some point be bound together to form a System Specification, or a separate System Specification may be written. Many systems, however, may not logically be broken down into smaller components because they are already broken down into the lowest common denominator. In these cases, a system document outline may be used to write a System Specification.

The System/Subsystem Specification is a technical document prepared for systems personnel. It is to be as detailed as possible concerning the environment and the design elements in order to provide maximum guidance to the program design effort. This document also defines system/subsystem interfaces. It is anticipated that the System/Subsystem Specification will present more detailed data than the FD due to the continuing design effort. However, it should be noted that any modification to the scope of the system effort should be submitted as a change to the FD. Subsystem Specifications consider only those segments of the FD that are applicable to the particular subsystem.

Program Specification (PS)

A PS (Program Specification) may be written after the SS (System/Subsystem Specification) to expand on its requirements or without any SS having been prepared. The PS may present modifications of the FD, but it should be noted that any modification to the scope of the system effort should be submitted as a change to the FD.

The PS is a technical document. The amount of detail to be included is dependent upon the use to be made of the document within the particular project for which it is prepared. The intent of a PS is to guide program development. It is anticipated that the PS will present more detailed data than the FD and the related SS as a result of the detailed program design effort. Furthermore, a PS will consider only those

segments of an FD or SS that are applicable to the particular program.

Data Base Specification (DS)

A DS (Data Base Specification) is generally prepared when many analysts/programmers will be involved in writing programs that will utilize the same data.

The DS is a technical document prepared for programmers. It is sufficiently detailed to permit program coding and data base generation by the development group. Since this document is intended to cover all types of systems, it does not make specific data or presentation formats mandatory. Developers of any given system are best qualified to devise the physical formats most useful and comprehensible to project personnel. However, to achieve consistency in documentation, the following practices apply in all Data Base Specifications:

1. Each graphic representation is to be followed by a narrative explanation.
2. Each item of information shown in a graphic representation is to be consistent with standardized data element names, as shown in data element libraries.

Users Manual (UM)

The primary purpose of the UM (Users Manual) is to serve the needs of the User Group. Sections 1 and 2 of the UM present general and specific information on a specific computer program system. They are directed toward an organization's general management and staff personnel who have no need for detailed technical information concerning system implementation or operation. Sections 3 and 4 of the UM address staff personnel but are more detailed in the discussions about how to provide input to the system; how to respond to requests from the system for information; and how to make use of outputs from the system that may be in the form of hard copy, CRT displays, or the like. Instructions for the operation of specific consoles or terminals may be included in sections 5 and 6. If a Users Manual is the only document produced for a particular computer program, an annotated program source listing must be provided.

Computer Operation Manual (OM)

The OM (Computer Operation Manual) contains precise and detailed information on the control requirements and operating procedures necessary to successfully initiate, run, and terminate the subject system. It is directed toward supervisory and operator personnel who are responsible for the efficient performance of their organization's computer center. These readers are interested primarily in detailed information on the external characteristics and operating procedures of a computer program. In general, the manual is written in a step-by-step fashion, as opposed to an expository style, in order to clarify and emphasize the procedures associated with the computer programs. Supporting illustrations are concerned with the flow of input data and output information but do not present breakdowns or delineations of the internal logic and flows within a computer program.

Program Maintenance Manual (MM)

The MM (Program Maintenance Manual) presents general and specific information on the computer program. It is written for personnel who are responsible for the maintenance of the computer programs. It describes the computer programs in a detailed, technical presentation to assist the maintenance programmer in functioning.

Test Plan (PT)

The PT (Test Plan) is a tool for directing the ADS testing and contains the orderly schedule of events and list of materials necessary to effect a comprehensive test of a complete ADS. Those parts of the document directed toward the staff personnel are presented in nontechnical language and those parts of the document directed toward the operations personnel are presented in suitable terminology.

Test Analysis Report (RT)

The RT (Test Analysis Report) describes the status of the computer program system after test completion and provides a presentation of deficiencies for review by staff and management personnel. Therefore, the document should be prepared in non-technical language.

Implementation Procedures (IP)

The IP (Implementation Procedures) is a tool for directing the installation or implementation of an ADS at locations other than the test site after testing of the ADS has been completed. It may also be used to direct the implementation of major modifications or enhancements of an ADS which has already been installed. Those parts of the document directed toward the staff personnel shall be presented in nontechnical language, and those parts of the document directed toward the operations personnel shall be presented in suitable terminology.

PROJECT DEVELOPMENT

The process of documentation is often identified as a separate phase of project development for accounting purposes. This gives the unfortunate impression that nothing need be done to write or prepare documents until the last stages of a phase of project development. It must be recognized by all personnel involved in project development, particularly the project manager, that documentation is a continuing part of the developmental effort. Additions to the draft documents should be made as frequently as possible to avoid the problem of preparing the necessary documents after programming has been completed. The documentation standards for the Navy have been arranged in a way that allows the evolutionary creation of the necessary portions of the supporting documents.

When it is anticipated that a document will be formalized for managerial review in the future, the evolutionary information should be added to the draft. The addition may take the form of a working paper in a notebook, developed in modular fashion as it becomes known.

DOCUMENT REDUNDANCY

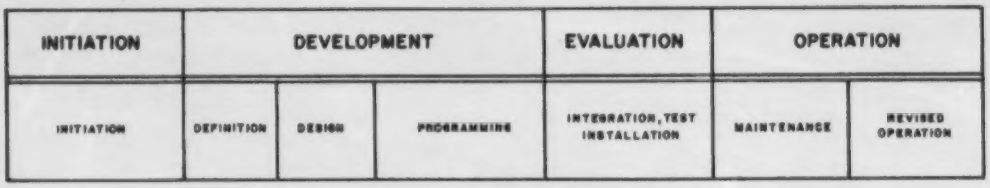
A comparison of the types of documents contained in the Documentation Standards will show a certain amount of redundancy. This redundancy is of two types. Introductory material has been included in each type of document to provide the reader with a frame of reference for reading the rest of the document. This information has been included because the overall philosophy of these types of documents is to provide "stand-alone" documents with a minimum of need for cross-referencing; however, cross-referencing is allowed. There is also apparent redundancy in that most types of documents specify that a description of inputs and outputs, a program summary, and the like, be included. The actual information that should be included for each of these items in the various types of documents is different; however, as the information is intended to be read by different audiences, it must, therefore, be prepared using the terminology that is suited to the appropriate audience. If, however, the audiences are essentially the same, cross-referencing is allowed.

ADS PROJECT LIFE CYCLE

Projects evolve through many phases of development between the time that an idea to create an ADS occurs and the time that a program can produce the needed output. A generalized development chart is shown in figure 7-10. Most of the phases shown are used on all program development efforts regardless of the size of the project. During project development, one phase may begin before the preceding phase has ended with little or no formal management review and evaluation at the beginning of each phase.

Initiation

Prior to beginning development, certain life cycle management planning actions must be accomplished. During the initiation phase, a



78.164

Figure 7-10.–A typical ADS development life cycle.

project request for the desired product is prepared. This project request may range from a verbal request to official correspondence, and specifies the objective or general capabilities being requested. Also included may be information on the point of contact for additional data, desired milestone dates, security classification, and environmental constraints. At this time, initial identification, justification, and validation are accomplished. As this information is generally specified in separate directives and is often limited by legal constraints if the services of a contractor are to be employed, no specification of the contents of the project request is included in these standards.

Development

During the development phase, which includes the definition, design, and programming stages, the project request is analyzed to determine alternative solutions and the best solution is selected depending on cost factors, timeliness of response, manpower availability, and other factors. If further ADS development is indicated, this solution is then designed, programmed, debugged, and tested.

Definition

During the definition stage, the proposed solution must be determined and the managerial techniques that will be used during the development must be planned. Included is a decision on whether or not a contractor will be used and, if so, for what stages (see DOD instruction 4100.33). Also included might be a determination of the documents that would be produced during the ADS life cycle.

A Functional Description is normally the only document produced during this stage. If the situation calls for the development of a Data Requirements Document, it may also be produced during this stage, but it is normally completed after the functional description. A document preparation chart is shown in figure 7-11 for each phase of an ADS project life cycle.

Design

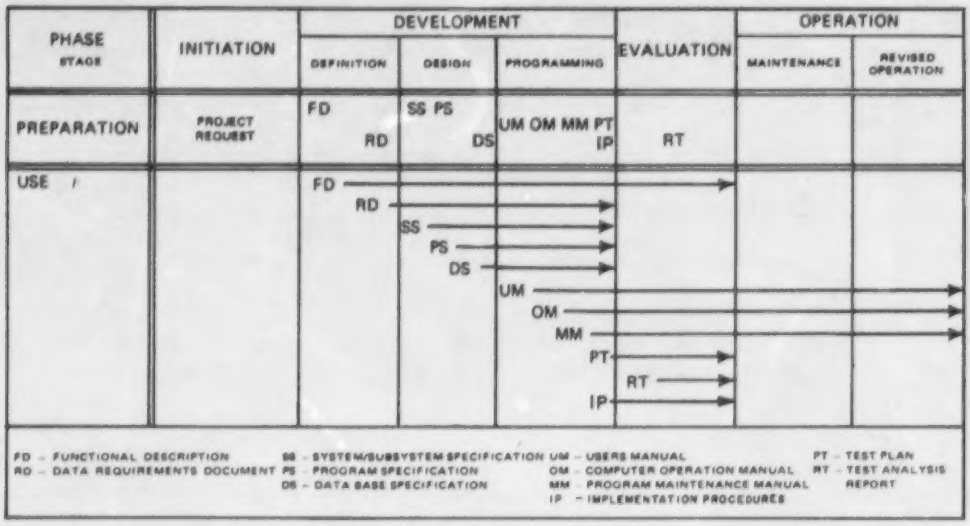
Following the definition stage, a design stage may be necessary if the project is relatively complex or is of sufficient size. This allows the creation of an intermediate milestone to ensure that the development is properly directed.

If this stage is necessary, a System/Subsystem Specification, Program Specification, and (if necessary) a Data Base Specification may be produced.

Programming

During the programming stage, a proposed solution created in either the definition or design stage is translated into computer instructions, the ADS is tested, and any errors are corrected.

During this stage the final documentation in the form of a Users Manual, a Computer Operation Manual, and a Program Maintenance Manual may be prepared. The Test Plan and the Implementation Procedures are also prepared in anticipation of the evaluation phase.



78.165

Figure 7-11.—A typical ADS development life cycle related to document preparation and use.

Evaluation

When the ADS development has reached this phase, the package of the completed programs and the related object documents are thoroughly reviewed to ensure their completeness and accuracy. During the evaluation phase, the computer program or system is run and reviewed by the personnel who requested its development in the project request to ensure that all requirements have been met. The organization(s) that will be responsible for the operation and maintenance of the program or system may also be consulted and given an opportunity to ensure that its requirements have been satisfied. Additionally, an implementation/installation date may be established.

The Test Analysis Report, if necessary, is prepared during this phase.

Operation

When the organizations mentioned in the preceding section are satisfied that their requirements have been met, the ADS becomes operational and is run as needed. Routine maintenance to meet changing operational requirements is performed and, to the extent required, some of the previous stages are repeated. This results in revisions to the ADS in the revised operation stage.

SUMMARY

Documentation is an extremely important facet of the data processing community. DP technical managers should ensure that all documentation developed under their supervision is prepared in accordance with the references cited in this chapter. Time and money can be saved if proper documentation standards are followed.

This chapter, appropriate appendixes, and referenced material should be reviewed by all DP2s and above prior to taking advancement in rate exams.

APPENDIX I

LIFE CYCLE PHASES AND POLICIES,

A. MISSION ANALYSIS/PROJECT INITIATION

1. The purpose of this phase is to identify a mission element need (set of functional requirements); validate that need; and recommend the exploration of alternative functional concepts to satisfy the need. This phase is completed upon approval of the Mission Element Need Statement at Milestone 0 at a prescribed organizational level and issuance of authority to explore and develop alternative concepts.

2. The following policies apply:

a. The Mission Element Need Statement (MENS) shall be prepared in accordance with SECNAVINST 5231.1 (Series).

b. When feasible, mission needs shall be satisfied through the use of existing DoD Component equipment and resources.

c. Information reporting requirements shall be justified and approved under the provisions of DoD Directive 5000.19.

d. DoD Component or OSD-directed requirements for standardization, integration, or interface with other automated information systems shall be accommodated. Such requirements will be explicitly identified and documented.

e. Appropriate measures to specify and safeguard vital management and operating information, and assure needed mobility, effectiveness, survivability and continuity of operations in peace and war shall be emphasized. This includes:

(1) Clearly identifying AIS wartime role, if any; and

(2) Designating secure backup facilities or making computers as transportable and as survivable as the principal activities which they support.

B. CONCEPT DEVELOPMENT

1. The purpose of this phase is to synthesize (or solicit) and evaluate alternative methods to accomplish the function shown in the approved MENS and to recommend one (or more) feasible concepts for further exploration. A determination is made whether several alternative concepts should be demonstrated or that demonstration should be omitted.

a. If demonstration is decided to be necessary, each functional concept selected for demonstration shall be outlined to the point that the function has been bounded and all risks stated. Competitive demonstrations are intended to verify that the chosen concepts are sound, could perform in an operational environment, and provide a basis for final selection of a concept.

b. During this phase, modeling and simulation of various concepts may be necessary to establish feasible functional baselines for further exploration. This phase is completed upon issuance of approval at Milestone 1 at a prescribed organizational level to demonstrate alternative concepts or to proceed directly to definition and design of an AIS based on a selected concept.

2. The following policies apply:

a. A project manager shall be designated during this phase for each major AIS and given authority to manage all aspects of the AIS. A project manager may be reassigned during the Concept Development, Definition/Design or System Development phases of a major AIS only with the express approval of senior functional and ADP officials. This provision is intended to promote continuity, responsibility and accountability.

b. An AIS to be used by more than one DoD Component shall be assigned to a DoD Component designated as Executive Agent and chartered by the Secretary of Defense.

c. Proposed constraints for the conduct of any demonstration and validation activity will be specified for each alternative. The constraints will establish the basis on which to continue or terminate the effort for each alternative through completion of the demonstration.

d. The interface of ADP, telecommunications and other supporting elements shall be recognized as an integral part of the AIS from the outset of planning and analysis efforts. Technical systems concepts, requirements, specifications and costs for communications assets shall be identified and coordinated with appropriate communications organizations during this phase and throughout the life cycle of each AIS in accordance with DoD Directive 4603.1.

e. Preliminary requirements for the protection of information shall be identified in this phase and refined during follow-on phases. Such requirements shall be in accordance with DoD Directives 5400.11 and 5200.28 and OMB Circular A-71, Transmittal Memorandum No. 1.

f. Necessary contractor versus in-house analysis shall be prepared in accordance with DoD Instruction 4100.33.

C. DEFINITION/DESIGN

1. The purpose of this phase is to define fully the functional requirements (system/subsystem specifications) and to design an operable AIS. This phase is completed when ADP and telecommunications technical adequacy has been validated and upon issuance of approval at Milestone II at a prescribed organizational level to develop fully the system.

2. The following policies apply:

a. Functional requirements and processes to be automated shall be documented and validated by an appropriate senior functional policy official before an AIS design is commenced. As a minimum, the functional documentation shall specify functional operational requirements and a detailed description of the function to be supported by automation.

b. Specific objectives expressed in terms of performance measures shall be established for each AIS project, supported by initial feasibility studies, and economic analyses prepared in accordance with DoD Instruction 7041.3 and refined in follow-on phases.

c. A new AIS may be designed only after it has been determined that an existing AIS, including one available from another DoD Component or off-the-shelf from industry, cannot be used or economically modified to satisfy validated functional requirements.

d. AIS designs shall exploit proven technology.

e. Each AIS shall be constructed in a modular structure providing a direct relationship of each module to the mission/function supported, unless another design technique is approved as more appropriate. As a goal, the overall AIS will be conceived and sized in a manner that will permit the development and evaluation of each module within 9 to 12 months after detailed design of the AIS has been completed. Such practices will contribute to logic visibility, reliability, maintainability, and reduce the risk and cost associated with evaluation and validation.

f. AIS design shall include provisions that will facilitate appropriate functional and technical audit of the AIS.

g. Requirements for specialized functional and technical training to operate an AIS, including associated time and costs, shall be identified in this time period and updated during follow-on phases. Proper coordination and adequate lead time for implementation shall be provided system users and training organizations.

D. SYSTEM DEVELOPMENT

1. The purpose of this phase is to develop, integrate, test and evaluate the ADP system and the total AIS. This phase is completed upon approval of the AIS by appropriate functional officials as satisfying the mission need; and issuance of approval at Milestone III at an appropriate organizational level to deploy and operate the approved AIS.

2. The following policies apply:

a. Each AIS development shall be supported by documented plans. The scope of ADP system life cycle management documentation shall be appropriate to the resource investment contemplated and consistent with the principles stated in this Directive and in DoD Instruction 7935.1 (Series).

b. Where an AIS must operate under both peacetime and wartime conditions, the development shall provide for immediate readiness and transition from one condition to the other without need for retrofit or redesign.

c. Modern software development concepts such as top down design, chief programmer teams, design walk-throughs and program libraries shall be used wherever practicable.

d. The DoD standard high order programing languages are specified in DoD Instruction 5000.31. The National Federal and/or DoD specifications for these languages shall be used. The use of specific DoD standard high order languages in AIS shall be based on the capabilities of the language to meet the system requirements as follows:

(1) Nonstandard high order programing languages may be used for classes of applications where, for technical reasons, the use of a DoD standard high order programing language would not be feasible. Such use shall be approved by the DoD Component Senior ADP Policy Official and an information copy of the determination shall be sent to the ASD(C).

(2) Machine dependent assembly languages may be used when the DoD standard high order programing language does not have the capability to accomplish required functions, and where it would not be cost beneficial to have the capabilities added to the DoD standard high order programing language compiler. Such use shall be approved by the DoD Component Senior ADP Policy Official and an information copy of the determination shall be sent to the ASD(C).

(3) Use of implementer defined features and vendor supplied nonstandard extensions in high order programing languages compilers shall be avoided.

e. A plan for continuity of operations shall be prepared for each AIS in accordance with DoD Directive 3020.26.

f. Any AIS, including those that will operate at multiple sites, shall be field tested at one (or more) representative operational sites, using actual functional transaction data, and shall be certified for adequacy by appropriate authority covering functional and technical interests prior to operation.

g. All components of the AIS (functional, ADP, and telecommunications requirements) shall be managed as configured items. The terms, tools and techniques contained in DoD Directive 5010.19 and those developed and approved by DoD Components shall be adopted or adapted for such configuration management of an AIS.

E. DEPLOYMENT AND OPERATION

1. The purpose of this phase is to (a) implement the approved operational plan, including extension/installation at other sites; (b) continue approved operations; (c) budget adequately; and (d) control all changes and maintain/modify the AIS during its remaining life using well defined configuration management procedures.

2. The following policies apply:

a. No AIS shall be made operational, including an AIS to be extended beyond its initial operation test site, without ensuring that the implementation plans, including training and resource availability, are sufficient to support the schedule for operations.

b. Computers designated as transportable field units shall be field tested periodically to assure that they can operate in field environments and that adequate power supplies and transportation support are available.

c. Each operational AIS shall be reevaluated on a periodic basis to assure that the AIS continues to operate efficiently and to meet functional requirements in a cost effective manner.

d. Prior to upgrading the ADPE of an AIS, the AIS shall undergo a performance evaluation and opportunities for sharing shall be explored.

e. An AIS which no longer serves a significant need shall be expeditiously terminated.

APPENDIX II

Users Manual AII-3

Computer Operation Manual AII-22

Program Maintenance Manual AII-27

USERS MANUAL
TABLE OF CONTENTS

		Page
SECTION 1.	GENERAL	1
1.1	Purpose of the Users Manual	1
1.2	Project References	1
1.3	Terms and Abbreviations	1
1.4	Security	1
SECTION 2.	SYSTEM SUMMARY	2
2.1	System Application	2
2.2	System Operation	2
2.3	System Configuration	2
2.4	System Organization	2
2.5	Performance	2
2.6	Data Base	3
2.7	General Description of Inputs, Processing, Outputs	4
SECTION 3.	STAFF FUNCTIONS RELATED TO TECHNICAL OPERATIONS	6
3.1	Initiation Procedures	6
3.2	Staff Input Requirements	6
3.2.1	Input Formats	7
3.2.2	Composition Rules	7
3.2.3	Input Vocabulary	8
3.2.4	Sample Inputs	8
3.3	Output Requirements	9
3.3.1	Output Formats	9
3.3.2	Sample Outputs	10
3.3.3	Output Vocabulary	10
3.4	Utilization of System Outputs	10
3.5	Recovery and Error Correction Procedures	10
SECTION 4.	FILE QUERY PROCEDURES	11
4.1	System Query Capabilities	11
4.2	Data Base Format	11
4.3	Query Preparation	11
4.4	Control Instructions	15

SECTION 5.		TERMINAL DATA DISPLAY AND RETRIEVAL PROCEDURES	16
	5.1	Available Capabilities	16
	5.2	Data Base Format	16
	5.3	Access Procedures	16
	5.4	Display and Retrieval Procedures	16
	5.5	Recovery and Error Correction Procedures	16
	5.6	Termination Procedures	16
SECTION 6.		TERMINAL DATA UPDATE PROCEDURES	17
	6.1	Frequency	17
	6.2	Restrictions	17
	6.3	Sources	17
	6.4	Access Procedures	17
	6.5	Update Procedures	17
	6.6	Recovery and Error Correction Procedures	17
	6.7	Termination Procedures	17

LIST OF FIGURES

Figures		Page
4-Ø1	Example of Preprogrammed Query Capability	12
4-Ø2	Example of Data Record Format	13
4-Ø3	Example of Query Card Format	14
4-Ø4	Example of Query Statement	14

SECTION 1. GENERAL

1.1 Purpose of the Users Manual. This paragraph shall describe the purpose of the UM (Users Manual) in the following words, modified when appropriate:

> The objective of the Users Manual for (Project Name) (Project Number) is to provide the user's non-ADP personnel with the information necessary to effectively use the system.

1.2 Project References. This paragraph shall provide a brief summary of the references applicable to the history and development of the project. The general nature of the computer programs (tactical, inventory control, war-gaming, management information, etc.) developed shall be specified. A brief description of the system shall include its purpose and uses. Also indicated shall be the project sponsor and user as well as the operating center(s) that will run the completed computer programs. At least the following documents, when applicable, shall be specified by author or source, reference number, title and security classification.

a. Project request.

b. Previously published documentation on the project.

c. Documentation concerning related projects.

d. Standards or reference documentation, such as:

(1) Documentation standards and specifications.

(2) Programming conventions.

(3) DoD or Federal standards (data elements, programing languages, etc.).

1.3 Terms and Abbreviations. This paragraph shall provide a list or include in an appendix any terms, definitions or acronyms unique to this document and subject to interpretation by the user of the document. This list will not include item names or data codes.

1.4 Security. This paragraph shall contain an overview and discussion of the security considerations associated with the data of the system.

SECTION 2. SYSTEM SUMMARY

2.1 System Application. The uses of the ADS in supporting the activities of the user's staff shall be generally stated and explained. The description shall include:

a. The purpose, reason, or rationale of the system.

b. Capabilities and operating improvements provided by the system.

c. Additional features, characteristics, and advantages considered appropriate in furnishing a clear, general description of the system and the benefits derived from it.

d. Functions performed by the system, such as preprocessing or postprocessing data input or output from a primary processor; maintenance of data files; display of submarine, surface or aircraft, etc.

2.2 System Operation. This paragraph will show the relationships of the functions performed by the system with the organizations or stations that are sources of input to the system and those that are recipients of output from it. Included shall be charts and a brief narrative description including only the who, what, where, and why concerning the inputs and outputs shown on the chart.

2.3 System Configuration. A brief narrative description of the equipment used by the system shall be given. It may include the type of computer and input and output devices.

2.4 System Organization. The objective of this paragraph shall be to present a general overview of the organization of the system. The presentation shall show, as appropriate, the logical parts of the system (such as subsystems and programs) and a brief description of their role in the operation of the system.

2.5 Performance. This paragraph shall present a brief description of the overall performance capabilities of the system, including how it meets the information requirements of the staff or how it supports associated activities. Performance measures and information of interest are represented by the following examples:

a. Input–Types, volumes, rate of inputs accepted.

b. Output–types, volume, accuracy, rate of outputs that the system can produce.

c. Response time–include qualifications, where necessary, that affect response time in processing operational reports, such as listing a tape, compiling an object program, etc. Type and volume of input and equipment configuration are examples of items that may influence running time and, consequently, response time.

d. Limitations–for example, maximum size per unit of input, format constraints, restrictions on what data files may be queried and by what location, language constraints.

e. Error rate–capabilities for detecting various legal and logical errors and the means provided for error correction.

f. Processing time–show typical processing times.

g. Flexibility–note provisions allowing extension of the usage of the system.

h. Reliability–note system provisions that support, for example, alternate processing or a switch-over capability.

2.6 Data Base. The data files that are referenced, supported, or kept current by the system shall be identified in functional terms. The brief description should include the type of data in the file and the usage made of it. If the system does not have a file query capability as described in Section 4, this paragraph will include a description of the data elements included in the data base. For each data element may be listed information such as the following:

a. Data element name

b. Synonymous name

c. Definition

d. Format

e. Range of values

f. Unit of measurement

g. Data item names, abbreviations and codes

When the information is published in a data element dictionary, reference to an entry in the dictionary will be made rather than including an

extract from that dictionary. Any variations in either the inputs or outputs from the format or data items that will be used on the data base of the ADS must be specifically identified.

2.7 General Description of Inputs, Processing, Outputs. This paragraph shall present a general narrative description of the inputs, the flow of data through the processing cycle, and the resultant outputs.

a. Inputs. In describing the inputs, consideration shall be given to the following:

(1) Purpose of input–explain why the input is made to the program system and note conditions or events requiring its submission.

(2) Content of input–describe what the input contains in the way of operational, control, or reference data.

(3) Associated inputs–describe any other inputs required by the system in addition to the direct input.

(4) Origin of inputs–identify the source or preparer of the input.

(5) Data files–identify in general or functional terms the data files associated with the input.

(6) Security considerations.

(7) Other–include additional remarks of general information.

b. Processing. In this paragraph, the relationship of the input to the output should be described with a general description of the flow of data through the processing cycle.

c. Outputs. In describing the outputs, consideration should be given to the following:

(1) Output–list the outputs produced by the program system showing their relationship to the inputs.

(2) Purpose of output–explain the reason for the output and note conditions or events that require its generation by the system.

(3) Content of output–describe in general terms the information provided by the output.

(4) Associated outputs–reference other system outputs that complement the information in this output.

(5) Distribution of outputs–note the recipients in the organization who receive this output.

(6) Security considerations.

(7) Other–describe additional items of general information.

SECTION 3. STAFF FUNCTIONS RELATED TO TECHNICAL OPERATIONS

Section 3 of the Users Manual shall provide the details necessary to prepare staff inputs to the system. The logical arrangement of the information shall enable the staff and functional personnel to prepare required inputs. In addition, this section will explain in detail the characteristics and meaning of the information the program system produces as outputs. If an exclusively batch processing system or an exclusively online system is being described, the following paragraphs should provide the necessary procedures for the staff to utilize the system. If an online system with batch processing capabilities is being described, this paragraph may reference the manual that describes the terminal operations and the following paragraphs may detail the procedures to be followed for the batch processing runs, or both may be presented herein. Optionally, the following information may be presented with each capability.

3.1 Initiation Procedures. The procedures that must be followed to initiate system operation will be detailed in this paragraph. Included may be information such as sample job request forms, sample control card formats, or log-on procedures to be used for Online terminal operations. If these procedures are standard or are detailed in another manual, that manual will be referenced.

3.2 Staff Input Requirements. The requirements to be observed in preparing entries to the program system shall be delineated in this paragraph for each different type or class of input. Typical considerations are the following:

a. Cause of input–note what operational conditions require the submission of the input (e.g., catastrophe, normal status report, need to enter parameters in a source program, need to update data, the desire to obtain particular data, the need to respond to a particular display).

b. Time of input–specify when the input must be prepared (e.g., periodically, randomly as a function of an operational situation).

c. Origin of input–identify the staff unit or station authorized to generate the input.

d. Medium of input–note the medium used to enter the input (e.g., keyboard, punched card, magnetic or paper tape).

e. Associated inputs – reference any related inputs that are required to be entered at the same time as this input.

f. Other – note any other applicable information, such as other recipients of the inputs; priority; security handling; variations on the basic input format using code or key indicators; limitations on what files may be interrogated by a particular type of input.

3.2.1 Input Formats. The layout form(s) used in the initial preparation of program system inputs shall be illustrated and the information which may be entered on the various sections and lines explained. The explanation of each entry provision shall be keyed to the sample form illustrated.

3.2.2 Composition Rules. This paragraph shall provide a description of the language and the grammatical rules and conventions that must be observed in order to prepare input that can be accepted by the program system. The rules of syntax, usage of punctuation, etc. will be explained. Items for consideration may include the following:

a. Input length–e.g., 1ØØ characters maximum.

b. Line length–e.g., 3Ø characters maximum.

c. Format–e.g., all input items must be left-justified.

d. Labeling–i.e., usage of tags or identifier to denote major data sets to the system.

e. Sequencing–i.e., the order and placement of items in the input.

f. Punctuation–i.e., spacing and use of symbols (virgule, asterisk, character combinations, etc.) to denote start and end of input, of lines, of data groups, etc.

g. Combination–i.e., rules forbidding use of particular character or parameter sets in an input.

3.2.3 Input Vocabulary. This paragraph shall explain the legal character combinations or codes that must be used to identify or compose input items.[1] Included may be codes for submission or operational status, inventory items, statements or operations.

3.2.4 Sample Inputs. Each class or type of input acceptable by the system shall be illustrated. An introduction will be given as to what the sample represents. A complete explanation shall follow, describing the significance of the subsections of the sample input. Included in the explanation may be information on the following types of inputs:

a. Header–containing entries that denote the input class or type, date/time, origin, instruction codes to the system, etc.

b. Text–containing the subsections of the input representing data for operational files, request parameters for an information retrieval program, etc.

c. Trailer–containing control data denoting the end of input and any additional control data.

d. Omissions–indicating those classes or types of input that may be omitted at the option of the composer or because of particular circumstances concerning the input.

e. Repeats–indicating those subsections of the input that may be repeated up to a specified maximum number of entries, if required.

[1] An appendix may be provided containing an alphabetical listing of item codes that can be entered into an input to the system or that can appear on an output from the system, and an alphabetical listing of functional or generic categories, e.g., materiel control, weather, ship type. Each of these basic categories will contain an alphabetical listing of associated data items and their code representation. If extensive lists of codes have previously been promulgated in final form, those lists shall be referenced.

3.3 Output Requirements. The requirements relevant to each class or type of output shall be described. Representative information that may be included for each class of output is:

a. Purpose–the reasons why the output is generated e.g., the desire to obtain particular data, due to the existence of an "exception" situation, to identify different operating units at different ranges.

b. Time–whether the output is randomly or periodically produced. If produced periodically, the period must be specified.

c. Options–any modifications or variations of the basic output that are available.

d. Media–physical form of the output, such as printout, CRT, tape, cards.

e. Location–where the output is required to appear, such as in the computer area or remotely at a particular physical area or station.

f. Other–any additional requirements for this output, such as priority, security handling, associated outputs that complement the information in this output.

3.3.1 Output Formats. The layout in which each class or type of system output is presented shall be explained in detail. Explanations shall be keyed to particular parts of the format illustrated. Appropriate information that may be provided includes the following:

a. Header–the title, identification, time, number of output parts, and similar basic control data that may be contained in the header or control segment of the output shall be described.

b. Body–the information that may appear in the body or text of the output must be explained. Described shall be the significance of fixed data, such as columnar headings in tabular display types of output. The existence of subsets or sections in the output format (e.g., part A, part B) should be noted. In card/tape output, the position or column locations allocated to specific output information should be described.

c. Trailer–the control or reference information that may be appended to the body of information presented shall be discussed.

Additional characteristics concerning the make-up of outputs may include information such as the meanings of special symbols, etc.

3.3.2 Sample Outputs. Illustrations of the output obtainable from the system shall be given for each different class or type. The function or purpose of the output shall be explained. A detailed description including information such as the following may be provided:

a. Definition–the meaning and use of each information variable for the reader or user.

b. Source–item extracted from a specific input, from a data base file, calculated by system, etc.

c. Characteristics–concerning omissibility of the item under certain conditions of the output generation, range of values, unit of measure.

3.3.3 Output Vocabulary. Any codes or abbreviations that appear in the output in a form different from those used on the input described in paragraph 3.2.3 shall be described in this paragraph.

3.4 Utilization of System Outputs. An explanation shall be given of the use of the output by the operational area or activity which receives it. For example, a summary report of POL (petroleum, oil, and lubricant) stocks may be received by a materiel control activity and, depending on the information in the report, action might be required to initiate the purchase or transfer of stocks to a particular location; the appearance of a blinking symbol on a CRT may require keyboard entries by several stations; etc.

3.5 Recovery and Error Correction Procedures. A list of the error codes generated by the application program and the corrective actions to be taken by the user to correct the condition shall be included within this paragraph. Also included in this paragraph shall be the procedures to be followed by the user to ensure that any recovery and restart capabilities can be utilized.

SECTION 4. FILE QUERY PROCEDURES

This section shall be prepared for those ADSs with a file query retrieval capability. The instructions necessary for recognition, preparation, and processing of a query applicable to the data base shall be cited in detail. The descriptive techniques illustrated in paragraphs 4.1, 4.2, and 4.3 shall be utilized as applicable.

4.1 System Query Capabilities. This paragraph shall illustrate in tabular form the preprogrammed query capabilities provided by the system with a cross-reference to a query card format or query statement. An example is shown in Figure 4-Ø1.

4.2 Data Base Format. This paragraph shall illustrate the data base format and content. An example is shown in Figure 4-Ø2. If applicable, the format shall show both the data which are not subject to queries and the data which, even though not specifically requested, are extracted for some queries. For each data element may be listed information such as the following:

a. Data element name

b. Synonymous name

c. Definition

d. Format

e. Range of values

f. Unit of measurement

g. Data item names, abbreviations and codes

When the information is published in a data element dictionary, reference to an entry in the dictionary will be made rather than including an extract from that dictionary. Any variations in either the inputs or outputs from the format or data items that are used on the data base must be specifically identified.

4.3 Query Preparation. Instructions shall be provided for the preparation of any necessary query title, request, and parameter input. The details of query input preparation in the context of each specific data base and system retrieval capability shall be repeated as necessary in the form of positive instructions. In cases when the retrieval capability is part of a support program system and query input formats are not needed, the specific query statement required shall be listed. Figure 4-Ø4 shows a specific query

QUERY	QUERY CARD FORMAT
Numbers of employees within an organization	A
Number of employees in a specific pay grade	B
Total gross pay for employees within an organization	C
State tax year to date for a specific state	D
FICA tax year to date for a specific employee	E
Total deductions for a specific employee	F
Net pay for a specific employee	G

FIGURE 4-01. Example of Preprogrammed Query Capability

ITEM NAME	RECORD POSITIONS	KIND OF DATA
ORG-NAME	1-30	Alpha-numeric
ORG-ID	31-36	Alpha-numeric
SOC-SEC-NO	37-45	Alpha-numeric
NAME	46-65	Alpha-numeric
PAY-GRADE	66-69	Alpha-numeric
GROSS-PAY	70-75	Signed-numeric
GROSS-PAY-YTD	76-89	Signed-numeric
FED-TAX	84-89	Signed-numeric
FED-TAX-YTD	90-97	Signed-numeric
FICA	98-103	Signed-numeric
FICA-YTD	104-111	Signed-numeric
STATE-TAX	112-117	Signed-numeric
STATE-TAX-YTD	118-125	Signed-numeric
STATE-TAX-CODE	126-127	Alpha-numeric
ALLOTMENTS	128-133	Signed-numeric
NET-PAY	134-139	Signed-numeric

FIGURE 4-02. Example of Data Record Format

FORMAT OF QUERY CARD A (NUMBER OF EMPLOYEES WITHIN AN ORGANIZATION)

QUERY ITEM TITLE	BEGIN IN CHAR. POS.	CONTENT/COMMENTS
Query Designator	1	Q Constant
File Number	2	01 Constant
Query Number	4	01 First Query
Security Classification	10	U Unclassified
Query Card Format Code	12	A
Organization	14	Insert ORG-ID Code as requested by query. Refer to data format for applicable code.

FIGURE 4-03. Example of Query Card Format

INFORMATION PROCESSING SYSTEM

Request–No. of employees within an organization (Office of Secretary of Defense)

Query Statement–IF ORG-ID EQ OSD LIST NO OF EMPLOYEES

FIGURE 4-04. Example of Query Statement

statement. The formats provided will be used by control personnel to transcribe queries into the technical phrasing of the retrieval system.

4.4 Control Instructions. Instruction shall be provided for the control of the sequencing of runs and of the program necessary to extract the response to the query request from the data base. These instructions shall include the requirements for, and the preparation of, control cards which may be required by the system or application programs. If extensive information concerning control card preparation is contained in support system documentation, this documentation may be referenced.

SECTION 5. TERMINAL DATA DISPLAY AND RETRIEVAL PROCEDURES

5.1 Available Capabilities. The data display and retrieval capabilities available through terminal operations will be stated and explained in general terms.

5.2 Data Base Content. This paragraph will discuss the content and, if applicable, the format of the data base used by the system with emphasis on the relationships among the data that can be displayed or retrieved.

5.3 Access Procedures. Presented in this paragraph will be the sequence of steps required to access the data base. Included will be such information as the name of the system or subsystem being called and other control information.

5.4 Display and Retrieval Procedures. Paragraphs 5.4.1 through 5.4.n will describe the step-by-step procedures necessary to produce the various displays and retrievals that are available through the use of a terminal. For each procedure information such as the name of the operation, input formats, and sample responses may be included.

5.5 Recovery and Error Correction Procedures. Error codes and messages should be provided indicating their meanings and any corrective actions that should be taken.

5.6 Termination Procedures. This paragraph will present the sequence of steps necessary to terminate the display or retrieval operation.

SECTION 6. TERMINAL DATA UPDATE PROCEDURES

6.1 Frequency. This paragraph will describe the frequency of data updates from terminals. Information such as the events that caused the update may be included.

6.2 Restrictions. This paragraph shall describe any restrictions on updating the data base. Included may be such factors as:

a. The offices or personnel authorized to update.

b. Time periods when such updating is allowed.

c. Information for ensuring that only authorized updates are allowed.

6.3 Sources. Included in this paragraph will be a list of the sources used to obtain the data that will make up each update.

6.4 Access Procedures. Presented in this paragraph will be the sequence of steps required to access the data base. Included will be such information as the name of the system or subsystem being called and other control information.

6.5 Update Procedures. Paragraph 6.5.1 through 6.5.n will provide information to enable an authorized user to update data in the system data base using a terminal. For each type of update procedure information such as the name of the operation, input formats, and sample responses may be included.

6.6 Recovery and Error Correction Procedures. Error codes and messages should be provided indicating their meanings and any corrective actions that should be taken. Any user initiated recovery procedures and validity checks should also be included in narrative form.

6.7 Termination Procedures. This paragraph shall present the step-by-step sequence of actions necessary to terminate the update.

COMPUTER OPERATION MANUAL
TABLE OF CONTENTS

SECTION 1.	GENERAL	1
1.1	Purpose of the Computer Operation Manual	1
1.2	Project References	1
1.3	Terms and Abbreviations	1
SECTION 2.	SYSTEM OVERVIEW	2
2.1	System Application	2
2.2	System Organization	2
2.3	Program Inventory	2
2.4	File Inventory	2
2.5	Processing Overview	2
2.6	Security	2
SECTION 3.	DESCRIPTION OF RUNS	3
3.1	Run Inventory	3
3.2	Phasing	3
3.3	Run Description (Identify)	3
3.3.1	Control Inputs	3
3.3.2	Management Information	3
3.3.3	Input-Output Files	4
3.3.4	Output Reports	4
3.3.5	Reproduced Output Reports	4
3.3.6	Restart/Recovery Procedures	5
3.4	Run Description (Identify)	5

SECTION 2. SYSTEM OVERVIEW

2.1 System Application. A brief description of the system including its purpose and uses shall be provided.

2.2 System Organization. This paragraph shall describe the operation of the system by use of a chart showing the data processing operations, including how the different operations are interrelated. If sets of runs are grouped by time periods or cycles, then each set of integrated operations required on a daily, weekly, etc. basis will be presented. If runs may be grouped logically by organizational level, the groups of runs that can be performed by each organizational level such as headquarters processing, field activity processing, etc., shall be presented.

2.3 Program Inventory. This paragraph shall provide an inventory of the various programs. This listing shall include the program full name, program ID, as well as security considerations of the programs and identification of those programs necessary to continue or resume operation of the ADS in case of an emergency.

2.4 File Inventory. This paragraph shall list all permanent files that are referenced, created, or updated by the system. This listing shall include information such as the file name, file ID, storage medium and required storage (number of tapes or disks) as well as security considerations. The listing shall also identify those files necessary to continue or resume operation of the ADS in case of an emergency.

2.5 Processing Overview. This paragraph will provide information which is applicable to the processing of the system. Separate paragraphs may be used as needed to cover system restrictions, waivers of operational standards, information oriented toward specific support areas (e.g., library, EAM support) or other processing requirements such as the following:

a. Interface with other systems.

b. Other pertinent system-related information.

2.6 Security. This paragraph shall contain an overview and discussion of the security considerations associated with the data of the system.

SECTION 3. DESCRIPTION OF RUNS

Section 3 of the Computer Operation Manual shall provide a description of the runs for operations and scheduling personnel to allow accurate and efficient scheduling of operations, assignment of equipment, the management of input and output data, and restart/recovery procedures. In online systems some information about system operational control will be related to the capabilities of the operating system and other information will need to be presented in a manner more directly useful to operators of online terminals. Much of the necessary information should be included in figures with additional information that is specifically oriented to the hardware and software set being used.

3.1 Run Inventory. This paragraph shall provide a list of the various runs (i.e., programs, jobs) that may be made by the system and include a brief summary of the purpose of the run. This list should relate to the runs that are included in the remainder of this section and should show the programs that are executed during the run.

3.2 Phasing. This paragraph shall provide a schedule of acceptable phasing of the program system into a logical series of operations. A system run may be phased to permit manual or semiautomatic checking of intermediate results, to provide the user with intermediate results for other purposes, or to permit a logical break if higher priority jobs are submitted. An example of the minimum division for most systems would be edit, file update, and report preparation.

3.3 Run Description (Identify). Paragraph 3.3 through 3.n will provide the detailed information needed to execute runs of the sytem. The information provided will be organized in a manner most useful to the operating centers and operations personnel that will perform the runs.

3.3.1 Control Inputs. This paragraph shall provide a listing of the runstream of job control statements needed to initiate the run.

3.3.2 Management Information. This paragraph shall present the information needed to manage the run including, for example, the following information:

a. Run identification.

b. Peripheral and resouce requirements.

c. Security considerations.

d. Method of initiation, such as on request, as a result of another run, at a predetermined time, etc.

e. Estimated run time.

f. Required turnaround time.

g. Messages and responses.

h. Procedures for taking check points.

i. Waivers from operational standards.

j. Contacts for problems experienced with the run.

3.3.3 Input-Output Files. This paragraph shall list information about the files that serve as input to or that are created or updated by the run. Included for each file should be information such as the following:

a. File name.

b. Security and privacy.

c. Recording medium.

d. Retention schedule.

e. Disposition of file.

3.3.4 Output Reports. This paragraph shall list information about the reports that are produced during the run. Included for each report should be information such as the following:

a. Report identification.

b. Security and privacy.

c. Medium (i.e., hardcopy, tape).

d. Volume of report.

e. Number of copies.

f. Distribution of copies.

3.3.5 Reproduced Output Reports. This paragraph shall provide information about those computer-generated reports that are subsequently reproduced by other means. Included for each report shall be information such as the following:

a. Report identification.

b. Security and privacy.

c. Reproduction technique.

d. Paper size.

e. Binding method.

f. Number of copies.

g. Distribution of copies.

3.3.6 Restart/Recovery Procedures. This paragraph shall provide information to the operations center personnel concerning restart/of a system failure.

3.4 Run Description (Identify). Paragraph 3.4 will present information about the second run in a manner similar to that used in paragraph 3.3.

PROGRAM MAINTENANCE MANUAL
TABLE OF CONTENTS

SECTION 1.	GENERAL DESCRIPTION	1
1.1	Purpose of the Program Maintenance Manual	1
1.2	Project References	1
1.3	Terms and Abbreviations	1
SECTION 2.	SYSTEM DESCRIPTION	2
2.1	System Application	2
2.2	Security	2
2.3	General Description	2
2.4	Program Description	2
SECTION 3.	ENVIRONMENT	5
3.1	Equipment Environment	5
3.2	Support Software	5
3.3	Data Base	5
3.3.1	General Characteristics	5
3.3.2	Organization and Detailed Description	5
SECTION 4.	PROGRAM MAINTENANCE PROCEDURES	7
4.1	Conventions	7
4.2	Verification Procedures	7
4.3	Error Conditions	7
4.4	Special Maintenance Procedures	7
4.5	Special Maintenance Programs	7
4.6	Listings	8

SECTION 1. GENERAL DESCRIPTION

1.1 Purpose of the Program Maintenance Manual. This paragraph shall describe the purpose of the MM (Program Maintenance Manual) in the following words or appropriate modifications thereto:

> The objective for writing this Program Maintenance manual for (Project Name) (Project Number) is to provide the maintenance programmer personnel with the information necessary to effectively maintain the system.

1.2 Project References. This paragraph shall provide a brief summary of the references applicable to the history and development of the project. The general nature of the system (tactical, inventory control, war-gaming, management information, etc.) developed shall be specified. A brief description of this sytem shall include its purpose and uses. Also indicated shall be the project sponsor and user as well as the operating center(s) that will run the completed computer programs. At least the following documents, when applicable, shall be specified by author or source, reference number, title and security classification:

a. Users Manual.

b. Computer Operation Manual.

c. Other pertinent documentation on the project.

1.3 Terms and Abbreviations. This paragraph shall provide a list or include in an appendix any terms, definitions or acronyms unique to this document and subject to interpretation by the user of the document. This list will not include item names or data codes.

SECTION 2. SYSTEM DESCRIPTION

2.1 System Application. The purpose of the system and the functions it performs shall be explained. A particular application system, for example, might serve to control mission activities by accepting specific inputs (status reports, emergency conditions), extracting items of data, and deriving other items of data in order to produce both information about a specific mission and information for summary reports. These functions shall be related to paragraphs 3.1, Specific Performance Requirements, and 4.2, System Functions, of the FD (Functional Description).

2.2 Security. This paragraph shall contain an overview and discussion of the security considerations associated with the data of the system.

2.3 General Description. This paragraph will provide a comprehensive description of the system, subsystem, jobs, etc. in terms of their overall functions. This description will be accompanied by a chart showing the interrelationships of the major components of the system.

2.4 Program Description. The purpose of this paragraph is to supply details and characteristics of each program and subroutine that would be of value to a maintenance programmer in understanding the program and its relationship to other programs. (Special maintenance programs related to the specific system being documented will be discussed under paragraph 4.4, Special Maintenance Procedures.) This paragraph will initially contain a list of all programs to be discussed, followed by a narrative description of each program and its respective subroutines under separate paragraphs starting with 2.4.1 through 2.4.n. For each major item listed below include any applicable information on security considerations. Information to be included in the narrative description is represented by the following items:

a. Identification–program title or tag, including a designation of the version number of the program.

b. Functions–description of program functions and the method used in the program to accomplish the function.

c. Input–description of the input. Description used here must include all information pertinent to maintenance programming including:

(1) Data records used by the program during operation.

(2) Input data type and location(s) used by the program when its operation begins.

(3) Entry requirements concerning the initiation of the program.

d. Processing–description of the processing performed by the program, including:

(1) Major operations–major operations of the program will be described. The description may reference chart(s) which may be included in an appendix. This chart will show the general logical flow of operations, such as read an input, access a data record, major decision, and print an output which would be represented by segments or subprograms within the program. Reference may be made to included charts that present each major operation in more detail.

(2) Major branching conditions provided in the program.

(3) Restrictions that have been designed into the system with respect to the operation of this program, or any limitations on the use of the program.

(4) Exit requirements concerning termination of the operation of the program.

(5) Communications or linkage to the next logical program (operational, control).

(6) Output data type and location(s) produced by the program for use by related processing segments of the system.

(7) Storage–Specify the amount and type of storage required to use the program and the broad parameters of the storage locations needed.

e. Output–description of the outputs produced by the program. While this description may reference output described in the Users Manual, any intermediate output, working files, etc., should be described for the benefit of the maintenance programmer.

f. Interfaces–description of the interfaces to and from this program.

g. Tables and Items–provide details and characteristics of the tables and items within each program. Items not part of a table must be

listed separately. Items contained within a table may be referenced from the table descriptions. If the data description of the program provides sufficient information, the program listing may be referenced to provide some of the necessary information. At least the following will be included for each table:

(1) Table tag, label or symbolic name.

(2) Full name and purpose of the table.

(3) Other programs that use this table.

(4) Logical divisions within the table (internal table blocks or parts–not entries).

(5) Basic table structure (fixed or variable length, fixed or variable entry structure).

(6) Table layout (a graphic presentation should be used). Included in supporting description should be table control information, details of the structure of each type of entry, unique or significant characteristics of the use of the table, and information about the names and locations of items within the table.

(7) Item–the term "item" refers to a specific category of detailed information that is coded for direct and immediate manipulation by a program. Used in this sense, the definition of an item is machine–and program-oriented rather than operationally oriented. Of primary importance is an explanation of the use of each item. At least the following will be included for each item:

(a) Item tag or label and full name.

(b) Purpose of the item.

(c) Item coding, depending upon the item type, such as integer, symbolic, status, etc.

h. Unique Run Features–description of any unique features of the running of this program that are not included in the Computer Operation Manual.

SECTION 3. ENVIRONMENT

3.1 Equipment Environment. This paragraph shall discuss the equipment configuration and its general characteristics as they apply to the system.

3.2 Support Software. This paragraph shall list the various support software used by the system and identify the version or release number under which the system was developed.

3.3 Data Base. Information in this paragraph shall include a complete description of the nature and content of each data base used by the system including security considerations.

3.3.1 General Characteristics. Provide a general description of the characteristics of the data base, including:

a. Identification–name and mnemonic reference. List the programs utilizing the data base.

b. Data Permanency–note whether the data base contains static data that a program can reference, but may not change, or dynamic data that can be changed or updated during system operation. Indicate whether the change is periodic or random as a function of input data.

c. Storage–specify the storage media for the data base (e.g., tape, disk, internal storage) and the amount of storage required.

d. Restrictions–explain any limitations on the use of this data base by the program in the system.

3.3.2 Organization and Detailed Description. This paragraph will serve to define the internal structure of the data base. A layout will be shown and its composition, such as records and tables, will be explained. If available, computer-generated or other listings of this detailed information may be referenced or included, herein. The following items indicate the type of information desired:

a. Layout–show the structure of the data base including records and items.

b. Sections–note whether the physical record is a logical record or one of several that constitute a logical record. Identify the record parts, such as header or control segments and the body of the record.

c. Fields–identify each field in the record structure and, if necessary, explain its purpose. Include for each field the following items:

   (1) Tags/labels–indicate the tag or label assigned to reference each field.

   (2) Size–indicate the length and number of bits/characters that make up each data field.

   (3) Range–indicate the range of acceptable value for the field entry.

d. Expansion–note provisions, if any, for adding additional data fields to the record.

SECTION 4. PROGRAM MAINTENANCE PROCEDURES

Section 4 of the manual shall provide information on the specific procedures necessary for the programmer to maintain the programs that make up the system.

4.1 Conventions. This paragraph will explain all rules, schemes, and conventions that have been used within the system. Information of this nature could include the following items:

a. Design of mnemonic identifiers and their application to the tagging or labeling of programs, subroutines, records, data fields, storage areas, etc.

b. Procedures and standards for charts, listings, serialization of cards, abbreviations used in statements and remarks, and symbols appearing in charts and listings.

c. The appropriate standards, fully identified, may be referenced in lieu of a detailed outline of conventions.

d. Standard data elements and related features.

4.2 Verification Procedures. This paragraph will include those requirements and procedures necessary to check the performance of a program section following its modification. Included may also be procedures for periodic verification of the program.

4.3 Error Conditions. A description of error conditons, not previously documented, may also be included. This description shall include an explanation of the source of the error and recommended methods to correct it.

4.4 Special Maintenance Procedures. This paragraph shall contain any special procedures required which have not been delineated elsewhere in this section. Specific information that may be appropriate for presentation would include:

a. Requirements, procedures, and verification which may be necessary to maintain the system input-output components, such as the data base.

b. Requirements, procedures, and verification methods necessary to perform a Library Maintenance System run.

4.5 Special Maintenance Programs. This paragraph shall contain an inventory and description of any special programs (such as file restoration,

purging history files) used to maintain the system. These programs should be described in the same manner as those described in the paragraphs 2.3 and 2.4 of the MM.

a. Input-Output Requirements. Included in this paragraph shall be the requirements concerning the equipment and materials needed to support the necessary maintenance tasks. Materials may, for example, include card decks for loading a maintenance program and the inputs which represent the changes to be made. When a support system is being used, this paragraph should reference the appropriate manual.

b. Procedures. The procedures, presented in a step-by-step manner, shall detail the method of preparing the inputs, such as structuring and sequencing of inputs. The operations or steps to be followed in setting up, running, and terminating the maintenance task on the equipment shall be given.

4.6 Listings. This paragraph will contain or provide a reference to the location of the program listing. Comments appropriate to particular instructions shall be made if necessary to understand and follow the listing.

INDEX

A

Abstract, document components, 7-6

Administration, data base, 5-3 to 5-11
  administrator functions, 5-4
  DBMS vs DMS, 5-6
  management tools for data elements (DED/D), 5-6 to 5-11

Administrator functions, data base, 5-4

ADP installations, 2-10 to 2-15
  equipment organization, 2-12
  nontactical ADP organization, 2-12 to 2-14
  nontactical ADP support, 2-15

ADP organization and personnel, 2-1 to 2-15
  ADP installations, 2-10 to 2-15
    equipment organization, 2-12
    nontactical ADP organization, 2-12 to 2-14
    nontactical ADP support, 2-15
  manpower authorizations, 2-4 to 2-10
    originating changes, 2-6 to 2-10
    requesting changes, 2-4 to 2-6
  manpower management, 2-1 to 2-3
    Chief of Naval Operations, 2-2
    how military manpower is acquired, 2-2 to 2-3
    manpower supporting organizations, 2-2
  personnel administration, 2-1
    responsibilities, 2-1

ADP physical security, risk management, and privacy, 3-1 to 3-33
  contingency planning, 3-17 to 3-22
    COOP preparation, 3-18 to 3-22
    COOP testing, 3-22

ADP physical security, risk management, and privacy—Continued
  data privacy, 3-26 to 3-33
    data risk assessment, 3-28 to 3-30
    data security risks, 3-30
    identification techniques, 3-33
    information management practices, 3-21 to 3-33
  natural disasters, 3-8 to 3-11
    fire safety, 3-8 to 3-11
  physical ADP protection, 3-13 to 3-17
    boundary protection, 3-14
    emanations, 3-14
    interior physical protection, 3-14
    physical security survey, 3-16 to 3-17
    remote terminal areas, 3-15
  physical security audits, 3-22 to 3-26
    audit follow-up, 3-26
    audit plan, 3-24
    audit preparation, 3-23
    conducting audits, 3-25
  physical security programs, 3-1 to 3-8
    ADP threats, 3-1
    implementing a security program, 3-7 to 3-8
    risk analysis, 3-2 to 3-7
  supporting utilities, 3-11 to 3-13
    electric power, 3-11 to 3-13

ADP threats, physical security, 3-1

ADPPRS, resource review and reports, 1-30 to 1-31

ADS project life cycle, 7-18 to 7-20
  definition, 7-19
  design, 7-19
  development, 7-19
  evaluation, 7-20
  initiation, 7-18
  operation, 7-20
  programming, 7-19

Analysis/decision (phase 3), systems analysis, 4-15 to 4-20
analysis of fact, 4-17
conclusions, 4-19
document and data collating, 4-17
recommendations, 4-19 to 4-20
Analysis generation, systems analysis, 4-6
Analysis study plan outline, 4-24 to 4-25
Annual loss expectancy, risk analysis, 3-4
Appendixes, document components, 7-11
Art of reprimanding, supervisory, 1-7
Audits, physical security, 3-22 to 3-26
conducting, 3-25
follow-up, 3-26
plan, 3-24
preparation, 3-23
Authoritative reference, security program, 3-7 to 3-8
Automated tools, description of, DED/D, 5-8

B

Back cover, document components, 7-13
Backup planning, COOP preparation, 3-20
Balanced supervision, 1-4
Boundary protection, physical ADP, 3-14

C

Communicating with upper management, 1-20
Components, document, 7-2 to 7-13
abstract, 7-6
appendixes, 7-11
back cover, 7-13
distribution list, 7-11
front cover, 7-3 to 7-5
index, 7-11
list of effective pages, 7-9 to 7-11
list of figures, 7-6
record of changes, 7-7, 7-9
special notices, 7-6
table of contents, 7-6
text, 7-11
title page, 7-6, 7-8
Computer Operation Manual, AII-22 to AII-26
Computer operation manual (OM), type of document, 7-17
Computer Performance Management (CPM) Program, instituting a, 1-21 to 1-26
CPM reporting, 1-22
evaluation and improvement, 1-22
improvement through evaluation, 1-23 to 1-25
use idle time productively, 1-25
management's role, 1-23
personnel evaluation, 1-25
program maintenance evaluation, 1-25 to 1-26
Contingency planning, 3-17 to 3-22
COOP preparation, 3-18 to 3-22
backup planning, 3-20
emergency response planning, 3-18 to 3-19
recovery planning, 3-21
COOP testing, 3-22
Control console, Series 6000, 6-15
Cooperation, elements to consider in developing, 1-9 to 1-10
Cooperation with your fellow supervisors, 1-11
Cooperation with your superior, 1-10 to 1-11
CPM and management responsibilities, 1-11 to 1-15
CPZ 300 card punch, Series 6000, 6-23
CRZ 301 card reader, Series 6000, 6-22

D

Data base organization, 5-1 to 5-17
data base administration, 5-3 to 5-11
administrator functions, 5-4
DBMS vs DMS, 5-6
management tools for data elements (DED/D), 5-6 to 5-11
data base management systems, 5-11 to 5-17
data manipulation languages (DMLs), 5-14
DMBS events, 5-14
schema, 5-12
schema and DML, 5-16
schema and storage schema, 5-17
schema DDL, 5-13
schema DDL and hardware, 5-15
schema/subschema data conversion, 5-16
subschemas, 5-12
definitions, 5-1 to 5-3

Data privacy, 3-26 to 3-33
data risk assessment, 3-28 to 3-30.
data security risks, 3-30
identification techniques, 3-33
information management practices, 3-31 to 3-33
assignment of responsibilities, 3-33
data processing practices, 3-32
handling of personal data, 3-31
maintenance of records to trace the disposition of personal data, 3-32
procedural auditing, 3-33
programming practices, 3-33
Data requirement document (RD), 7-16
DBMS events, 5-14
DBMS vs DMS, data base administration, 5-6
DED/D relationship to DBMS, 5-9 to 5-10
DED/D, summary on, 5-10 to 5-11
Definitions, data base organization, 5-1 to 5-3
Data element dictionary/directory, 5-8
Design, systems analysis, 4-20 to 4-23
data base design and specifications, 4-22
input design specifications, 4-21
output design specifications, 4-20
processing rules and specifications, 4-22 to 4-23
Development of cooperation, supervisory, duty, 1-3
Development of morale, supervisory duty, 1-3
Discipline, management, 1-6 to 1-7, 1-8
human relations aspect, 1-8
maintaining, 1-6 to 1-7
positive and negative, 1-8
Distribution list, document components, 7-11
DMLs, data manipulation languages, DBMS, 5-14
Document redundancy, 7-18
Documentation preparation and standards, 7-1 to 7-20
document components, 7-2 to 7-13
abstract, 7-6
appendixes, 7-11
back cover, 7-13
distribution list, 7-11
front cover, 7-3 to 7-5
index, 7-11
list of effective pages, 7-9 to 7-11
list of figures, 7-6
record of changes, 7-7, 7-9
special notices, 7-6
Documentation preparation and standards—Continued
document components—Continued
table of contents, 7-6
text, 7-11
title page, 7-6, 7-8
document documentation requirements, 7-13 to 7-15
need for standard documentation, 7-1
project development, 7-18 to 7-20
ADS project life cycle, 7-18 to 7-20
document redundancy, 7-18
summary, 7-20
types of documents, 7-15 to 7-18
computer operation manual (OM), 7-17
data base specification (DS), 7-17
data requirement document (RD), 7-16
functional description, (FD), 7-15
implementation procedures (IP), 7-18
program maintenance manual (MM), 7-17
program specification (PS), 7-16
system/subsystem specification (SS), 7-16
test analysis report (RT), 7-18
test plan (PT), 7-17
users manual (UM), 7-17
DS, data base specification, document, 7-17
DSS181B disk storage sybsystem, Series 6000, 6-16 to 6-17

E

Effective pages, list of, document components, 7-9 to 7-11
Electric power, supporting utilities, 3-11 to 3-13
Emanations, physical ADP protection, 3-14
Emergency response planning, COOP preparation, 3-18 to 3-19
Equipment organization, ADP installations, 2-12
Evaluation and improvement, CPM, 1-22
Experience, systems analyst, 4-4

F

FD, functional description, type of document, 7-15

Figures, list of, document components, 7-6
FIPS acquisition, 1-30
Fire safety, natural disasters, 3-8 to 3-11
facility fire exposure, 3-8
fire detection, 3-9
fire extinguishment, 3-10 to 3-11
Front cover, document components, 7-3 to 7-5

G

GCOS, General Comprehensive Operating Supervisor, Honeywell, 6-4 to 6-6
batch processing, 6-4
File Management Supervisor (FMS), 6-4
interactive remote job entry, 6-5
message switching, 6-5
on-line document handler, 6-5
remote processing, 6-5
time sharing, 6-5
Total Online Testing System (TOLTS), 6-6
transaction processing, 6-5

H

Hardware overview, Honeywell computer, 6-6 to 6-10
functional modularity, 6-6
Input/Output Multiplexer (IOM), 6-9 to 6-10
memory module, 6-7
processor module, 6-8
Honeywell computer, WWMCCS, 6-3 to 6-23
General Comprehensive Operating Supervisor (GCOS), 6-4 to 6-6
hardware overview, 6-6 to 6-10
remote input/output operations, 6-10 to 6-12
Series 6000 characteristics, 6-13 to 6-23

I

Identification techniques, data privacy, 3-33
Implementation (phase 5), systems analysis, 4-23 to 4-24
development, 4-23
research, 4-23
testing, 4-24
user approval, 4-24
Improvement through evaluation, CPM 1-23 to 1-25
Index, document components, 7-11
Information management practices, data privacy, 3-31 to 3-33
assignment of responsibilities, 3-33
data processing practices, 3-32
handling of personal data, 3-31
maintenance of records to trace the disposition of personal data, 3-32
procedural auditing, 3-33
programming practices, 3-33
Initiative, supervisory, 1-5 to 1-6
Interior physical protection, ADP, 3-14
J-SIIDS components, 3-15
Interpersonal skills, job analyst, 4-5
Interview/survey (phase 2), systems analyst, 4-11 to 4-15
document and data collection, 4-15
interviewing, 4-12 to 4-15
problem survey, 4-11
IP, implementation procedures, 7-18

J

Job description, systems analyst, 4-3
J-SIIDS components, interior physical protection, ADP, 3-15

L

Life cycle phases and policies, AI-1 to AI-5
Loss potential estimates, risk analysis, 3-2

M

Magnetic tape subsystems, Series 6000, 6-17 to 6-19
Management systems, data base, 5-11 to 5-17
data manipulation languages (DMLs), 5-14
DBMS events, 5-14
schema, 5-12
schema and DML, 5-16
schema and storage schema, 5-17
schema DDL, 5-13
schema DDL and hardware, 5-15
schema/subschema data conversion, 5-16
subschemas, 5-12

Management techniques, 1-1 to 1-31
instituting a Computer Performance Management (CPM) Program, 1-21 to 1-26
CPM reporting, 1-22
evaluation and improvement, 1-22
improvement through evaluation, 1-23
management's role, 1-23
personnel evaluation, 1-25
program maintenance evaluation, 1-25 to 1-26
manager position, 1-11 to 1-21
communicating with upper management, 1-20
CPM and management responsibilities, 1-11 to 1-15
production control and scheduling, 1-19
resource management, 1-19 to 1-20
scheduling, 1-15 to 1-19
user support, 1-19
vendor relations, 1-21
resource review and reports, 1-26 to 1-31
ADPPRS, 1-30 to 1-31
FIPS acquisition, 1-30
management's source material, 1-26 to 1-30
supervisory position, 1-1 to 1-11
achieving teamwork within your own group, 1-9 to 1-10
art of reprimanding, 1-7
common mistakes, 1-2
cooperation with your fellow supervisors, 1-11
cooperation with your superior, 1-10 to 1-11
duties and responsibilities, 1-2 to 1-4
fine line, the, 1-2
human relations aspect of discipline, 1-8
initiative, 1-5 to 1-6
maintaining discipline, 1-6 to 1-7
positive and negative discipline, 1-8
traits of a good supervisor, 1-4 to 1-5
Management tools for data elements, (DED/D), 5-6 to 5-11
data element dictionary/directory, 5-8
DED/D relationship to DBMS, 5-9 to 5-10
description of automated tools, 5-8
primary DED/D, 5-9
secondary DED/D, 5-10
summary on DED/D, 5-10 to 5-11
Management's role, CPM 1-23
Management's source material, 1-26 to 1-30
Manager position, 1-11 to 1-21
communicating with upper management, 1-20
CPM and management responsibilities, 1-11 to 1-15
user requirements, 1-12 to 1-15
production control and scheduling, 1-19
resource management, 1-19 to 1-20
scheduling, 1-15 to 1-19
by shift, 1-19
operations, 1-16 to 1-19
run scheduling, 1-19
user support, 1-19
vendor relations, 1-21
Manpower authorizations, ADP, 2-4 to 2-10
originating changes, 2-6 to 2-10
new OPNAV Form 1000/2, 2-6
officer and enlisted billet changes, 2-6
short format for requesting minor changes, 2-6
personnel requirements, 2-7 to 2-10
requesting changes, 2-4 to 2-6
administrative chain of command, 2-4 to 2-6
Manpower management, ADP, 2-1 to 2-3
Chief of Naval Operations, 2-2
how military manpower is acquired, 2-2 to 2-3
manpower supporting organizations, 2-2
MM, program maintenance manual, type of document, 7-17

N

Natural disasters, 3-8 to 3-11
fire safety, 3-8 to 3-11
facility fire exposure, 3-8
fire detection, 3-9
fire extinguishment, 3-10 to 3-11
Navy hardware/software users, 6-2 to 6-3
NCA, National Command Authorities, 6-1
NMCS, National Military Command System, 6-1
Notices, special, document components, 7-6

O

OM, computer operation manual, type of document, 7-17
Originating changes, manpower authorizations, 2-6 to 2-10
  new OPNAV Form 1000/2, 2-6
  officer and enlisted billet changes, 2-6
  short format for requesting minor changes, 2-6

P

Peripheral subsystems, Series 6000, 6-15
Personnel administration, ADP, 2-1
  responsibilities, 2-1
Personnel evaluation, CPM, 1-25
Personnel requirements, manpower authorizations, 2-7 to 2-10
Physical ADP protection, 3-13 to 3-17
  boundary protection, 3-14
  emanations, 3-14
  interior physical protection, 3-14
    J-SIIDS components, 3-15
  physical security survey, 3-16 to 3-17
  remote terminal areas, 3-15
Physical security audits, 3-22 to 3-26
  audit follow-up, 3-26
  audit plan, 3-24
  audit preparation, 3-23
  conducting audits, 3-25
Physical security programs, 3-1 to 3-8
  ADP threats, 3-1
  implementing a security program, 3-7 to 3-8
    authoritative reference, 3-7 to 3-8
  risk analysis, 3-2 to 3-7
    annual loss expectancy, 3-4
    loss potential estimates, 3-2
    selecting remedial measures, 3-5 to 3-7
    threat analysis, 3-3
Preparation, COOP, 3-18 to 3-22
Preparation (phase 1), system analysis, 4-8 to 4-11
  analysis study commencement, 4-11
  analysis study plan, 4-9
  approval, 4-8
  interview forms, 4-10
  interview schedule coordination, 4-11
  questionnaires, 4-10
Preparation (phase 1), system analysis—Continued
  schedules, 4-9
  scope, 4-9
  study team indoctrination, 4-10
  team appointment, 4-9
Primary DED/D, 5-9
Production control and scheduling, manager position, 1-19
Production, supervisory, 1-3
Program maintenance evaluation, 1-25 to 1-26
Program Maintenance Manual, AII-27 to AII-35
Program Maintenance Manual (MM), type of document, 7-17
Project development, documentation, 7-18 to 7-20
  ADS project life cycle, 7-18 to 7-20
    definition, 7-19
    design, 7-19
    development, 7-19
    evaluation, 7-20
    initiation, 7-18
    operation, 7-20
    programming, 7-19
  document redundancy, 7-18
  summary, 7-20
PRT 303 printer, Series 6000, 6-21
PS, program specification, type of document, 7-16
PT, test plan, type of document, 7-17

R

RD, data requirement document, 7-16
Record of changes, document components, 7-7, 7-9
Recovery planning, COOP preparation, 3-21
Remedial measures, selecting, risk analysis, 3-5 to 3-7
Remote input/output operations, Honeywell computer, 6-10 to 6-12
  DATANET 355 front-end network processor, 6-11 to 6-12
  remote processing capabilities, 6-10
Remote terminal areas, physical ADP, 3-15

Requesting changes, manpower authorizations, 2-4 to 2-6
administrative chain of command, 2-4 to 2-6
Requirements, document documentation, 7-13 to 7-15
Reports and records, supervisory, 1-4
Resource management, 1-19 to 1-20
Resource review and reports, 1-26 to 1-31
ADPPRS, 1-30 to 1-31
FIPS acquisition, 1-30
management's source material, 1-26 to 1-30
Responsibilities, personnel administration, ADP, 2-1
Risk analysis, physical security, 3-2 to 3-7
annual loss expectancy, 3-4
loss potential estimates, 3-2
selecting remedial measures, 3-5 to 3-7
threat analysis, 3-3
Risk assessment, data, 3-28 to 3-30
RT, test analysis report, type of document, 7-18

S

Safety, health, and physical welfare, supervisory duty, 1-3
Scheduling, manager position, 1-15 to 1-19
by shift, 1-19
operations, 1-16 to 1-19
run scheduling, 1-19
Schema and DML, DBMS, 5-16
Schema and storage schema, DBMS, 5-17
Schema, DBMS, 5-12
Schema DDL and hardware, DBMS, 5-15
Schema DDL, DBMS, 5-13
Schema/subschema data conversion, DBMS, 5-16
Secondary DED/D, 5-10
Security program, implementing a, 3-7 to 3-8
authoritative reference, 3-7 to 3-8
Security risks, data, 3-30
Security survey, physical, ADP, 3-16 to 3-17
Series 6000 characteristics, Honeywell computer, 6-13 to 6-23
control console, 6-15
CPZ 300 card punch, 6-23
CRZ 301 card reader, 6-22
DSS181B disk storage subsystem, 6-16 to 6-17
magnetic tape subsystems, 6-17 to 6-19
Series 6000 characterestics, Honeywell computer—Continued
peripheral subsystems, 6-15
PRT303 printer, 6-21
URC001 and URC002 unit record controls, 6-19 to 6-21
SS, system/subsystem specification, type of document, 7-16
Subschemas, DBMS, 5-12
Supervisory position, 1-1 to 1-11
achieving teamwork within your own group, 1-9
art of reprimanding, 1-7
common mistakes, 1-2
cooperation with your fellow supervisors, 1-11
cooperation with your superior, 1-10 to 1-11
keeping the boss informed, 1-10 to 1-11
make suggestions tactfully, 1-10
duties and responsibilities, 1-2 to 1-4
balanced supervision, 1-4
development of cooperation, 1-3
development of morale, 1-4
production, 1-3
reports and records, 1-4
safety, health, and physical welfare, 1-3
training and development of subordinates, 1-4
elements to consider in developing cooperation, 1-9 to 1-10
correcting mistakes, 1-9
delegation of responsibility and authority, 1-9
giving credit, 1-10
keeping your people informed, 1-9
setting the example, 1-10
tactful handling of personal problems, 1-10
fine line, the, 1-2
human relations aspect of discipline, 1-8
initiative, 1-5 to 1-6
confidence, 1-6
decisiveness, 1-5
fairness, 1-5
sincerity and integrity, 1-5
tact and courtesy, 1-5

Supervisory position—Continued
maintaining discipline, 1-6 to 1-7
art of giving orders, 1-6
individual, 1-6 to 1-7
situation, 1-6
positive and negative discipline, 1-8
traits of a good supervisor, 1-4 to 1-5
genuine interest in people, 1-4 to 1-5
loyalty, 1-4
positive thinking, 1-4
Supporting utilities, 3-11 to 3-13
electric power, 3-11 to 3-13
Systems analysis, 4-1 to 4-25
definitions, 4-1 to 4-2
phases of a system anlaysis study, 4-7 to 4-24
analysis/decision (phase 3), 4-15 to 4-20
analysis study plan outline, 4-24 to 4-25
analysis study team, 4-8
design (phase 4), 4-20 to 4-23
implementation (phase 5), 4-23 to 4-24
interview/survey, (phase 2), 4-11 to 4-15
preparation (phase 1), 4-8 to 4-11
systems analyst, 4-2 to 4-6
analysis generation, 4-6
experience, 4-4
interpersonal skills, 4-5
job description, 4-3
systems analysis, 4-5

T

Table of contents, document components, 7-6
Teamwork, achieving, within in own group, 1-9
Test analysis report (RT), type of document, 7-18
Test plan (PT), type of document, 7-17
Testing, COOP, 3-22
Text, document components, 7-11
Threat analysis, risk analysis, 3-3
Title page, document components, 7-6, 7-8
Training and development of subordinates, supervisory, 1-4
Traits of a good supervisor, 1-4 to 1-5
Types of documents, 7-15 to 7-18
computer operation manual (OM), 7-17
data base specification (DS), 7-17
data requirement document (RD), 7-16
functional description (FD), 7-15
implementation procedures, (IP), 7-18
program maintenance manual (MM), 7-17
program specification (PS), 7-16
system/subsystem specification (SS), 7-16
test analysis report (RT), 7-18
test plan (PT), 7-17
users manual (UM), 7-17

U

UM, Users Manual, type of document, 7-17
URC001 and URC002 unit record controls, Series 6000, 6-19 to 6-21
User support, management position, 1-19
Users Manual, AII-3 to AII-21

V

Vendor relations, manager position, 1-21

W

Worldwide Military Command and Control System operations community, 6-1 to 6-23
Honeywell computer, 6-3 to 6-23
General Comprehensive Operating Supervisor (GCOS), 6-4 to 6-6
hardware overview, 6-6 to 6-10
remote input/output operations, 6-10 to 6-12
Series 6000 characteristics, 6-13 to 6-23
National Command Authorities, (NCA), 6-1
National Military Command System (NMCS), 6-1
Navy hardware/software users, 6-2 to 6-3
Worldwide Miltary Command and Control System (WWMCCS), 6-2
WWMCCS, Worldwide Military Command and Control System, 6-2

DATA PROCESSING TECHNICIAN 1&C

NAVEDTRA 10265-D

Prepared by the Naval Education and Training Program Development Center, Pensacola, Florida

---

Your NRCC contains a set of assignments and perforated answer sheets. The Rate Training Manual, Data Processing Technician 1 & C NAVEDTRA 10265-D , is your textbook for the NRCC. If an errata sheet comes with the NRCC, make all indicated changes or corrections. Do not change or correct the textbook or assignments in any other way.

HOW TO COMPLETE THIS COURSE SUCCESSFULLY

Study the textbook pages given at the beginning of each assignment before trying to answer the items. Pay attention to tables and illustrations as they contain a lot of information. Making your own drawings can help you understand the subject matter. Also, read the learning objectives that precede the sets of items. The learning objectives and items are based on the subject matter or study material in the textbook. The objectives tell you what you should be able to do by studying assigned textual material and answering the items.

At this point you should be ready to answer the items in the assignment. Read each item carefully. Select the BEST ANSWER for each item, consulting your textbook when necessary. Be sure to select the BEST ANSWER from the subject matter in the textbook. You may discuss difficult points in the course with others. However, the answer you select must be your own. Remove a perforated answer sheet from the back of this text, write in the proper assignment number, and enter your answer for each item.

Your NRCC will be administered by your command or, in the case of small commands, by the Naval Education and Training Program Development Center. No matter who administers your course you can complete it successfully by earning a 3.2 for each assignment. The unit breakdown of the course, if any, is shown later under Naval Reserve Retirement Credit.

WHEN YOUR COURSE IS ADMINISTERED BY LOCAL COMMAND

As soon as you have finished an assignment, submit the completed answer sheet to the officer designated to grade it. The graded answer sheet will not be returned to you.

If you are completing this NRCC to become eligible to take the fleetwide advancement examination, follow a schedule that will enable you to complete all assignments in time. Your schedule should call for the completion of at least one assignment per month.

Although you complete the course successfully, the Naval Education and Training Program Development Center will not issue you a letter of satisfactory completion. Your command will make an entry in your service record, giving you credit for your work.

WHEN YOUR COURSE IS ADMINISTERED BY THE NAVAL EDUCATION AND TRAINING PROGRAM DEVELOPMENT CENTER

After finishing an assignment, go on to the next. Retain each completed answer sheet until you finish all the assignments in a unit (or in the course if it is not divided into units). Using the envelopes provided, mail your completed answer sheets to the Naval Education and Training Program Development Center where they will be graded and the score recorded. Make sure all blanks at the top of each answer sheet are filled in. Unless you furnish all the information required, it will be impossible to give you credit for your work. The graded answer sheets will not be returned.

The Naval Education and Training Program Development Center will issue a letter of satisfactory completion to certify successful completion of the course (or a creditable unit of the course). To receive a course-completion letter, follow the directions given on the course-completion form in the back of this NRCC.

You may keep the textbook and assignments for this course. Return them only in the event you disenroll from the course or otherwise fail to complete the course. Directions for returning the textbook and assignments are given on the book-return form in the back of this NRCC.

PREPARING FOR YOUR ADVANCEMENT EXAMINATION

Your examination for advancement is based on the Occupational Standards for your rating as found in the MANUAL OF NAVY ENLISTED MANPOWER AND PERSONNEL CLASSIFICATIONS AND OCCUPATIONAL STANDARDS (NAVPERS 18068). These Occupational Standards define the minimum tasks required of your rating. The sources of questions in your advancement examination are listed in the BIBLIOGRAPHY FOR ADVANCEMENT STUDY (NAVEDTRA 10052). For your convenience, the Occupational Standards and the sources of questions for your rating are combined in a single pamphlet for the series of examinations for each year. These OCCUPATIONAL STANDARDS AND BIBLIOGRAPHY SHEETS (called Bib Sheets), are available from your ESO. Since your textbook and NRCC are among the sources listed in the bibliography, be sure to study both as you take the course. The qualifications for your rating may have changed since your course and textbook were printed, so refer to the latest edition of the Bib Sheets.

NAVAL RESERVE RETIREMENT CREDIT

The course is evaluated at 12 Naval Reserve retirement points, which will be credited upon satisfactory completion of the entire course. These points are creditable to personnel eligible to receive them under current directives governing the retirement of Naval Reserve Personnel. Credit cannot be given again for this course if the student has previously received credit for completing another Data Processing Technician 1 & C course.

COURSE OBJECTIVE

In completing this NRCC, you will demonstrate a knowledge of the subject matter by correctly answering questions on the following:

principles of good supervision; responsibilities of the data processing manager; guidelines used in establishing service, management, and operational objectives

instituting a Computer Performance Management program; the management of ADP resources; personnel acquisition; delineating personnel responsibilities; requesting changes to manpower authorizations

conducting a physical security audit of an ADP facility; requirements of the Privacy Act of 1974 in handling personnel data

personnel skills required for billet structure allowance; characteristics of ADP installations in the Navy; risk analysis procedures; security measures

methods of fire safety, detection, and extinguishment; electric power utility problems; developing and implementing contingency plans

steps in a systems analysis procedure; ADP terms; problems and objectives in systems analyses; phases in a systems analysis

conducting personnel interviews; assembling information for decision making; data management systems and data base management systems

creating, managing, and manipulating data base software tools; functions of software tools utilized in a DBMS; command structures associated with the WWMCCS operations community

operations of the General Comprehensive Operating Supervisor in the WWMCCS Honeywell Computer; hardware characteristics of the WWMCCS Honeywell Computer; remote input/output operations of the WWMCCS Honeywell Computer

documentation as related to ADP in the Navy and SECNAVINST 5233.1 (Series); components of each documentation manual; characteristics of each document type and function; aspects of project development

While working on this correspondence course, you may refer freely to the text. You may seek advice and instruction from others on problems arising in the course, but the solutions submitted must be the result of your own work and decisions. You are prohibited from referring to or copying the solutions of others, or giving completed solutions to anyone else taking the same course.

Naval courses may include a variety of questions -- multiple-choice, true-false, matching, etc. The questions are not grouped by type; regardless of type, they are presented in the same general sequence as the textbook material upon which they are based. This presentation is designed to preserve continuity of thought, permitting step-by-step development of ideas. Some courses use many types of questions, others only a few. The student can readily identify the type of each question (and the action required) through inspection of the samples given below.

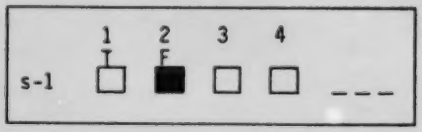
MULTIPLE-CHOICE QUESTIONS

Each question contains several alternatives, one of which provides the best answer to the question. Select the best alternative, and blacken the appropriate box on the answer sheet.

SAMPLE

s-1. The first person to be appointed Secretary of Defense under the National Security Act of 1947 was
1. George Marshall
2. James Forrestal
3. Chester Nimitz
4. William Halsey

Indicate in this way on the answer sheet:



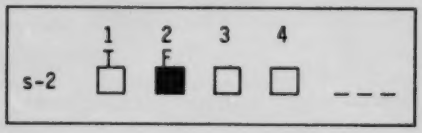
TRUE-FALSE QUESTIONS

Mark each statement true or false as indicated below. If any part of the statement is false the statement is to be considered false. Make the decision, and blacken the appropriate box on the answer sheet.

SAMPLE

s-2. Any naval officer is authorized to correspond officially with any systems command of the Department of the Navy without his commanding officer's endorsement.

Indicate in this way on the answer sheet:



MATCHING QUESTIONS

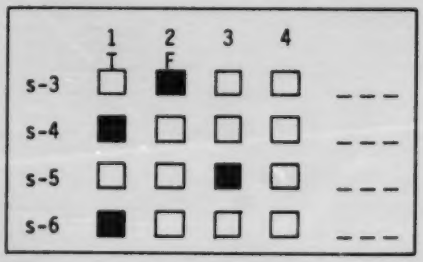
Each set of questions consists of two columns, each listing words, phrases or sentences. The task is to select the item in column B which is the best match for the item in column A that is being considered. Items in column B may be used once, more than once, or not at all. Specific instructions are given with each set of questions. Select the numbers identifying the answers and blacken the appropriate boxes on the answer sheet.

SAMPLE

In questions s-3 through s-6, match the name of the shipboard officer in column A by selecting from column B the name of the department in which the officer functions.

A	B
s-3. Damage Control Assistant	1. Operations Department
s-4. CIC Officer	2. Engineering Department
s-5. Disbursing Officer	3. Supply Department
s-6. Communications Officer	

Indicate in this way on the answer sheet:



Assignment 1

DP Supervision and Management

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 1-1 through 1-19

Learning Objective: Identify the principles and practices of good supervision, pointing out mistakes which supervisors sometimes make.

1-1. The ADP supervisor should continuously measure and evaluate the facility performance in support of established

1. personnel wants and desires
2. management wants and desires
3. personnel goals and objectives
4. management goals and objectives

QUESTIONS 1-2 THROUGH 1-5 ARE TO BE JUDGED TRUE OR FALSE.

1-2. The ADP term "user" is defined as a person who abuses ADP resources.

1. True
2. False

1-3. A good supervisor knows how to get the most out of the crew and still be sensitive to their human needs.

1. True
2. False

1-4. If a supervisor were to apply enough pressure on a crew, the production rate would be permanently increased.

1. True
2. False

1-5. A high level of production indicates good supervision only when it is accomplished willingly and with interest on the part of the crew.

1. True
2. False

1-6. Which of the following actions should a DP1 or DPC take upon assuming duties as a supervisor?

1. Make it clear that all things will be changed
2. Tell the crew that from now on, no foolishness will be tolerated
3. Tell the crew that things will stay the same for the present
4. Make the crew feel good by indicating that something will be done about all of their gripes

1-7. As a new supervisor on the job, a DP1 or DPC will be able to keep matters better in hand by following which of the following practices?

1. Trust none of the subordinates
2. Accept none of the responsibility for the crew's mistakes
3. Give orders that will not be questioned by the crew
4. Accept full responsibility for anything that takes place on the job

1-8. Which of the following practices should a supervisor follow in building the proper relationship with the crew?

1. Make it clear by certain actions that the supervisor is a step above the crew
2. Have answers for everything, and make it clear that suggestions are not needed
3. Be like one of the crew, both on and off the job
4. Maintain a friendly, conservative manner, be consistent, demonstrate confidence in the crew, and set a good example

1-9. The supervisor must follow which of the following practices to ensure that work is done properly and is accomplished on time?

1. Organize the work
2. Delegate as much authority as is feasible
3. Supervise and control the work
4. Do all of the above

QUESTION 1-10 IS TO BE JUDGED TRUE OR FALSE.

1-10. Since a supervisor's concern for the health and welfare of the crew pays dividends in the form of increased procuction, the supervisor should plan every stage of a project with safety in mind and set a good example by following safety practices.

1. True
2. False

1-11. Effective teamwork in an organization demands which of the following types of cooperation on the part of the supervisor?

1. Cooperation with the Members of the staff
2. Cooperation with the Other supervisors
3. Cooperation with the supervisor's superior
4. All of the above

1-12. A productive crew has which of the following characteristics?

1. A lot of liberty
2. High morale
3. Numerous medals
4. A light workload

1-13. Which of the following is a good supervisory practice that is common to all positions?

1. Maintaining a casual relationship with subordinates
2. Training and developing subordinates
3. Delegating no authority to subordinates
4. Disregarding suggestions by subordinates in major decisions

1-14. To be successful, a supervisor must strive for balanced supervision by following which of the following practices?

1. Stressing safety as the most important factor in the job
2. Allotting the major portion of time to personnel matters
3. Emphasizing training as the most important attribute to a creditable production record
4. Placing the proper stress on each of the responsibilities

1-15. Loyalty is one of the most important traits of a good supervisor. Which of the following statements demonstrates the best means to instill loyalty?

1. Maintain a "buddy-buddy" relationship with the crew
2. Insist that the crew "do as I say, not as I do"
3. Believe and practice the maxim "loyalty encourages loyalty"
4. Each of the above

1-16. Which of the following characteristics would NOT be found in a positive-thinking leader?

1. Displaying indifference to changes
2. Looking to the future with confidence
3. Going about the daily routine with enthusiasm
4. Taking advantage of new ideas and training opportunities

1-17. Which of the following steps should a new supervisor take first?

1. Have the crew get hair cuts
2. Give the crew a personnel inspection
3. Get to know the crew personally
4. Give the whole crew special liberty

1-18. Which of the following is characteristic of a person with initiative?

1. An open and alert mind
2. Continually looking for a better way to do things
3. Correcting unsafe conditions before accidents occur
4. Each of the above

QUESTIONS 1-19 AND 1-20 ARE TO BE JUDGED TRUE OR FALSE.

1-19. When a problem arises that involves many factors worthy of consideration, the supervisor should still be prompt in making a decision and risk the possibility of overlooking some of those factors.

1. True
2. False

1-20. Courtesy and fairness are important qualities for a DP1 or DPC.

1. True
2. False

USE THE FOLLOWING INFORMATION ON THE ACTIONS AND TRAITS OF FOUR DATA PROCESSING CHIEFS IN ANSWERING QUESTION 1-21.

CHIEF MOON DISMISSES TRIFLES AS OF NO IMPORTANCE; HE WILL RELAX WITH SOME OF THE CREW BUT NOT WITH OTHERS; HE EXHIBITS A BOLD FRONT TO SUBORDINATES.
CHIEF KNIGHT IS WARM AND FRIENDLY; HE IS ENTHUSIASTIC ABOUT HIS JOB; HE IS ALWAYS LOOKING FOR A BETTER WAY TO DO THINGS.
CHIEF DAY PLACES LITTLE SIGNIFICANCE IN CREW SENTIMENT; SHE BELIEVES IN "BEARING DOWN" WHEN THINGS GET LAX; SHE IS ALWAYS THE DOMINANT PERSONALITY IN A GROUP.
CHIEF STARR LEAVES DECISIONS TO HIS SUPERIOR; HE SHOWS INTEREST IN HIS SUBORDINATES; HE WAITS TO SEE WHAT OTHER SUPERVISORS WILL DO ABOUT COMMON PROBLEMS.

1-21. Which of the four DPCs show characteristics that are usually most desirable in a supervisor?

1. Knight
2. Day
3. Starr
4. Moon

Learning Objective: Specify the principles and techniques of giving orders and reprimands.

QUESTIONS 1-22 AND 1-23 ARE TO BE JUDGED TRUE OR FALSE.

1-22. A supervisor who deals with personnel squarely and honestly all the time will win and hold their respect.

1. True
2. False

1-23. A supervisor who possesses a quiet inner confidence usually has a cocky manner.

1. True
2. False

1-24. What is the minimum number of basic types of orders available to a supervisor?

1. 1
2. 2
3. 3
4. 4

1-25. Which of the following factors determine(s) the words used in giving an order?

1. Rate of the person to whom the order is given
2. Personality of the individual to whom the order is given
3. Situation under which the order is given
4. All of the above

1-26. Assume a crew member has been seriously injured and you want Seaman Jones to call an ambulance. Which of the following orders should you use?

1. "Jones, call the ambulance."
2. "Jones, will you call the ambulance please?"
3. "Jones, perhaps we should call the ambulance."
4. Either 2 or 3, but not both

1-27. Which of the following types of orders is recommended for a DP1 or DPC to use when supervising a group of normal, average people who are doing routine tasks?

1. Direct command
2. Request
3. Suggestion
4. Each of the above

1-28. The suggestion type of order is appropriate when it is directed toward which of the following types of individual?

1. One who has initiative and likes to work independently
2. One who is lazy and insubordinate
3. One who lacks initiative but is otherwise a good worker
4. One who is careless and indifferent to orders

1-29. Which of the following statements is usually true with respect to the request type of order?

1. It has authority over other types of orders
2. It demands initiative, especially when a person does not like to work independently
3. It tends to create a feeling of cooperation and teamwork
4. It is not recommended for the normal person

QUESTIONS 1-30 AND 1-31 ARE TO BE JUDGED TRUE OR FALSE.

1-30. The tone of voice in which you give an order is immaterial as long as you use the correct words.

1. True
2. False

1-31. The reprimand is the most commonly used form of disciplinary action and should be fitted to the individual and the situation.

1. True
2. False

1-32. What is the first step to be taken when you reprimand a person?

1. Ask the person why the error was made
2. Get the person to admit making the mistake
3. Get all the facts in the case
4. Call the person down on the spot

1-33. To test the effectiveness of your reprimand, ask yourself which of the following questions?

1. "Did it instill fear in the crew?"
2. "Did it cause regret on the part of the person who erred?"
3. "Did it build morale?"
4. Both 2 and 3 above

1-34. The basis for true discipline is the spirit of

1. freedom
2. cooperation
3. indifference
4. apathy

1-35. What type of motivation is produced in a crew by the practice of negative discipline?

1. Esprit de corps of the crew
2. Desire to increase production
3. Desire to cooperate
4. Fear of reprisal

1-36. Which of the following human relations factors does NOT contribute to a positive disciplinary program?

1. Knowing each individual in the group
2. Admitting errors if made
3. Frequently showing authority
4. Refraining from the use of authority to accomplish objectives

1-37. Which of the following actions is most typical of an approach to a policy of positive discipline by a supervisor?

1. Insist that action be taken in cases of minor disciplinary infractions as well as in major cases
2. Utilize idle time for training activity whenever possible
3. Retain authority for the accomplishment of delegated functions
4. Investigate the veracity of statements of subordinates

QUESTION 1-38 IS TO BE JUDGED TRUE OR FALSE.

1-38. In pursuing a positive approach to discipline, a supervisor reduces the need for formal discipline by removing as many causes of misconduct as possible.

1. True
2. False

Learning Objective: Identify the elements of teamwork that are necessary in an organization and determine methods of achieving teamwork.

1-39. Which of the following psychological factors is/are necessary in achieving teamwork within a group?

1. A feeling of security
2. A feeling of pride
3. A feeling of "being somebody"
4. All of the above

1-40. Which of the following objectives is basic to the goal of achieving teamwork?

1. Procurement of qualified personnel
2. Effective management in the field of human relations
3. Good working conditions
4. Performance equivalent to cost outlay for personnel

1-41. The principal obstacles to establishing a genuinely cooperative spirit with fellow supervisors are usually which of the following conditions?

1. Competition for jobs and unrealistic deadlines
2. Friction and jealousy
3. Large workloads
4. Misunderstandings

1-42. Unless safety is involved, which of the following supervisors should directly correct a mistake a crew member is making?

1. The chief in charge of the facility
2. The crew member's immediate supervisor
3. The commanding officer of the facility
4. The executive officer of the facility

QUESTIONS 1-43 THROUGH 1-45 ARE TO BE JUDGED TRUE OR FALSE.

1-43. A supervisor should never let crew members know all the reasons why a task has to be completed a certain way.

1. True
2. False

1-44. Frequent and sincere praise is an incentive to a crew as a whole.

1. True
2. False

1-45. A supervisor should never give advice to a crew member involving the member's personal problems at work.

1. True
2. False

1-46. Which of the following qualities is usually the most desirable in a crew member?

1. Punctuality
2. Loyalty
3. Neatness
4. Durability

1-47. In the interest of cooperation, which of the following means should be used to keep your supervisor informed?

1. Reporting everything that is said by personnel during the day
2. Reporting all errors that have occurred during the day
3. Reporting those personnel who fail to keep tidy work spaces
4. Reporting personnel problems that exist and any changes in work procedures that you intend to make

1-48. Which of the following is/are (an) obstacle(s) in establishing cooperation with fellow supervisors?

1. Seniority and pride
2. Idiosyncrasy
3. Friction and jealousy
4. Temperament

Learning Objective: Recognize some of the functions and responsibilities of the data processing manager.

1-49. Which of the following responsibilities is/are (a) function(s) of the data processing manager?

1. Applying the most economical contract terms
2. Assuring proper computations of rental and maintenance costs
3. Recording of time and obtaining the most effective use of equipment
4. All of the above

1-50. Which of the following descriptions is pertinent to a Computer Performance Management (CPM) program?

1. A software program that computes octal numbers
2. A program that evaluates the performance of an installed computer system
3. A program that evaluates local upper management
4. A program that evaluates all ADP facilities

1-51. Which of the following factors has sometimes turned the ADP facility technical manager's job into an overwhelming challenge?

1. Leadership responsibilities
2. Management responsibilities
3. Personal problems
4. Computer technology

Learning Objective: Determine some of the information guidelines used in establishing service, management, and operational objectives for ADP installations.

1-52. The decisions that the ADP facility technical manager faces nearly every workday includes which of the following factors?

1. What improvements could be realized by minor modifications to user requirements
2. If user complaints about poor service are justified
3. How should the computer room be laid out to optimize operator efficiency
4. All of the above

1-53. Which of the following time blocks is known as prime time hours?

1. 0001 to 0700
2. 0700 to 1600
3. 1600 to 2000
4. 2000 to 2400

1-54. Which of the following actions go hand-in-hand in the control, operation, and financial budgeting of an ADP facility?

1. Supervision and management
2. Leadership and restrictions
3. Command and control
4. Scheduling and teaching

1-55. To whom is ADP management's greatest responsibility?

1. The operator
2. The programmer
3. The user
4. The analyst

QUESTIONS 1-56 AND 1-57 ARE TO BE JUDGED TRUE OR FALSE.

1-56. Personally surveying users is a practical approach to defining such requirements as turnaround time.

1. True
2. False

1-57. Turnaround time evaluation should be obtained from information contained in the system accounting log files.

1. True
2. False

1-58. The user requirement termed "accessibility" is most closely related to

1. locating remote processors and terminals to use
2. anticipating a system crash
3. relying on the computer to meet deadlines
4. scheduling computer time during operational periods

1-59. Which of the following practices on a computer system should be avoided during prime work hours?

1. Fire drills
2. Two-hour blocks of scheduled time
3. Three hours of unscheduled time
4. Complete single project system dedication

1-60. A computer schedule should allow time for which of the following procedures?

1. Manual operations
2. Set-up time
3. Unavoidable delays
4. All of the above

1-61. What time factor should be introduced into a schedule to compensate for coordination variances?

1. Lead time
2. Lag time
3. Maintenance time
4. Buffer time

1-62. By which of the following means does intelligent programming inherently help to reduce setup time associated with large computer system operations?

1. Eliminating the need of scheduling program testing time
2. Keeping to a minimum the number of changes of tape reels required
3. Keeping to a minimum the total number of instructions in a program
4. Using the most efficient program instructions possible

1-63. What information does figure 1-3 in your textbook indicate regarding tape unit 2?

1. Tape unit 2 was used for regular job mix and other than regular job mix
2. Tape unit 2 was used 9 hours for regular job mix, 2 hours for scheduled maintenance, and 4 hours for other than regular job mix
3. Tape unit 2 was used 8 hours for regular job mix, 1 hour for scheduled maintenance, and 6 hours for other than regular job mix
4. Tape unit 2 was used 15 hours for regular job mix

1-64. What is the normal relationship between processor time and I/O time?

1. The processor time is twice the I/O time
2. The I/O time is twice the processor time
3. The I/O time is equal to the processor time
4. The processor time is four times the I/O time

1-65. For which of the following reasons should allocations of time be made when operations are scheduled?

1. Special requests
2. Unscheduled maintenance
3. Reruns
4. All of the above

1-66. On which of the following time measures should a preliminary schedule be devised?

1. Daily
2. Weekly
3. Monthly
4. Quarterly

1-67. You need the answers to numerous questions in order to develop a fairly accurate preliminary schedule of data processing operations. Which of the following purposes would be the primary reason to ask the question, "What is the relationship of one application to another?

1. To learn the relative priorities of data processing procedures
2. To learn whether it is possible to consolidate setup functions for different operations
3. To determine the relative processing times of the different procedures
4. To determine the relative program testing times for the different procedures

1-68. Programmers are able to estimate the running time of each program they prepare. You can use such estimates in scheduling computer operations after you modify them to include the time required for

1. equipment setup and the input and output of data
2. equipment setup and error recovery provisions
3. error recovery provisions and the input and output of data
4. input and output of data

1-69. What method(s) is/are used in most installations to establish the actual schedule?

1. Priority system
2. Normal frequency
3. Demand
4. A combination of the above

IN QUESTIONS 1-70 THROUGH 1-73, MATCH THE CATEGORIES OF TIME IN COLUMN A WITH THE DEFINITION OF TIME IN COLUMN B. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

A. CATEGORY TIME	B. DEFINITION
1-70. Production time	1. Time used for program testing
1-71. Assembly time	2. Time used for processing an application
1-72. Testing time	3. Time used for program assembly or compilation
1-73. Training time	4. Time used for training operation or programming personnel

1-74. Which of the following events should be recorded in the log under buffer time?

1. Assembly of programs
2. Unpredictable events that occur during processing
3. Training personnel
4. Reprocessing operations that are due to faulty input media

1-75. What scheduling method should be used to inform a user when to expect delivery of a run?

1. Run scheduling
2. Demand scheduling
3. Scheduling by shift
4. Scheduling by control

Assignment 2

ADP Resources and Personnel Management

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 1-19 through 2-19

2-1. What information is furnished the section supervisor when the scheduling-by-shift method is used?

1. Setup time and completion time of each individual operation
2. Start time of each individual operation and when the operation must be completed
3. Number of runs to be completed during the shift only
4. Start time for each run only

2-2. When utilizing shift scheduling, which of the following individuals is responsible for detailed scheduling?

1. The DP technical manager
2. The user
3. The shift supervisor
4. The console operator

2-3. Which of the following is/are the net result(s) of a good production control and scheduling system?

1. Reduction in cost
2. Responsive to the user
3. Both 1 and 2 above
4. Elimination of time consuming program checkout

2-4. The ADP facility technical manager's most obvious responsibility is the direct control of

1. fire drills
2. resources
3. training lectures
4. programming standards

2-5. Which of the following solutions is recommended for cutting cost of an ADP operation?

1. Cutback of civil service overtime
2. Reduction in operator shifts
3. Tight control of supplies
4. All of the above

2-6. Preferably, status reports should be submitted to upper management in what format?

1. Hand written
2. Graphical
3. Computer type
4. Crayon

2-7. Which of the following guidelines should be followed when reports are written for upper management?

1. Reports should be comprehensive with minimum graphics
2. Reports should provide a comparison of the facility's current performance level against a set of predefined goals
3. The amount of information reported should exceed upper management requirements for decision making
4. All of the above

2-8. The terms and conditions of a maintenance contract must be applied with care to ensure the best interest of the

1. Navy
2. DP technical manager
3. Commanding Officer
4. user

2-9. Which of the following procedures is currently being followed regarding the expansion of maintenance responsibilities for ADP equipments?

1. Joint, contractor/user clauses are written into all contracts
2. The contractor is solely responsible for all maintenance
3. The Navy, in certain situations, is responsible for maintenance
4. The user is responsible for maintenance in all new contracts

Learning Objective: Recognize some of the procedures involved in instituting a Computer Performance Management program.

2-10. When each phase of a life cycle of a system is reported, which of the following practices is/are recommended?

1. The data types should be determined according to availability
2. The report should remain highly visible when completed
3. The report should provide a historical trend
4. Both 2 and 3 above

2-11. Which of the following factors is a reliable indicator of the baseline system's natural reaction to various workload demands?

1. Future requirements
2. Equipment type
3. Site conditions
4. Past performance

2-12. Which, if any, of the following statements pertains to the data requirements specified by SECNAVINST 10462.18?

1. Most ADP facilities require less utilization data than the report requires
2. Most ADP facilities require more utilization data than the report requires
3. SECNAVINST 10462.18 does not specify format for reports
4. None of the above

2-13. Which of the following individuals should play a central role in instituting and overseeing a CPM program?

1. The DP technical manager
2. The lead programmer
3. The tape librarian
4. The shift supervisor

2-14. In determining the need for reports, any CPM program should

1. undergo a periodic review at least bi-annually
2. reflect changes in informational needs in new CPM reports
3. examine existing reports to establish historical trends

2-15. Which of the following is the most usual form of rental rates for ADP equipment?

1. Straight hourly rates
2. Straight monthly rates
3. Standard monthly rates for a specified number of hours and extra charges for overtime machine usage
4. Variable monthly rates determined according to the average number of hours of actual machine usage

2-16. Many tasks are performed by the operator and the computer. Which of the following functions is usually performed by the computer?

1. Judgement
2. Repetitive
3. Control
4. Evaluation

2-17. Of what relative importance is the human efficiency factor in EAM and ADPS operations?

1. Equally important because machines are unable to recognize errors
2. More important in EAM because EAMs depend wholly on manual control and data handling
3. More important in ADPS because the operating speeds of ADPS magnify and compound human errors immediately
4. More important in EAM because EAMs lack the complex automatic control and checking features of the ADPS

2-18. In which of the following ways can the operating standards of a data processing installation be raised?

1. By instituting a continuous on-the-job training programs
2. By having the operating manuals accessable to operators
3. By using idle machin time for productive purposes
4. Each of the above

QUESTIONS 2-19 THROUGH 2-21 ARE TO BE JUDGED TRUE OR FALSE.

2-19. The use of idle machine time is more easily controlled for EAM than EDP systems.

1. True
2. False

2-20. When evaluating a new operator, the number of errors made on a computer system is more important than the amount of improvement made.

1. True
2. False

2-21. Skill and experience must be taken into consideration when evaluating the efficiency of programmers.

1. True
2. False

2-22. Which of the following statements could be justification to change a production program?

1. Additional output needs
2. I/O format changes
3. Obsolete requirements
4. All of the above

2-23. Once a program is released for production, after final review, and found acceptable under operating conditions, it must then be completely

1. streamlined
2. stored on disk
3. documented
4. rewritten in FORTRAN

2-24. The section or division charged with program maintenance should maintain a master copy of each run manual for which of the following reasons?

1. To provide a ready reference for operators
2. To facilitate the preparation of new run manuals
3. To prevent the loss or destruction of program instructions
4. Both 2 and 3 above

Learning Objective: Identify the instructions and standards relevant to the management of ADP resources and reporting.

IN QUESTIONS 2-25 THROUGH 2-28, MATCH THE INSTRUCTION TITLE IN COLUMN B WITH THE SECNAVINST NUMBER IN COLUMN A.

	A. SECNAVINST NUMBER	B. INSTRUCTION TITLE
2-25.	5231.1	1. ADP Review and Evaluation Program
2-26.	5238.1	2. Government-Wide ADP Sharing Program
2-27.	10462.16	3. ADP Program Reporting System
2-28.	10462.18	4. Management of ADS Development

2-29. The use of FIPS was approved in SECNAVINST

1. 5200.28 series
2. 5230.3 series
3. 5238.1 series
4. 10462.16 series

IN ITEMS 2-30 THROUGH 2-33, MATCH THE FIPS PUB TITLE IN COLUMN B WITH THE FIPS PUB NUMBER IN COLUMN A.

	A. FIPS PUB NUMBER	B. FIPS PUB TITLE
2-30.	11-1	1. DICTIONARY FOR INFORMATION PROCESSING
2-31.	21-1	2. GUIDELINE ON COMPUTER PERFORMANCE MANAGEMENT: AN INTRODUCTION
2-32.	35	3. COBOL
2-33.	49	4. CODE EXTENSION TECHNIQUES IN 7 OR 8 BITS

IN QUESTIONS 2-34 THROUGH 2-37, MATCH THE FIPS PUB TITLE IN COLUMN B WITH THE FIPS PUB NUMBER IN COLUMN A.

	A. FIPS PUB NUMBER	B. FIPS PUB TITLE
2-34.	1	1. COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974
2-35.	3-1	2. CODE FOR INFORMATION INTERCHANGE
2-36.	24	3. RECORDED MAGNETIC TAPE FOR INFORMATION INTERCHANGE (800 CPI, NRZI)
2-37.	41	4. FLOWCHART SYMBOLS AND THEIR USAGE IN INFORMATION PROCESSING

ITEMS 2-38 AND 2-39 ARE TO BE JUDGED TRUE OR FALSE.

2-38. All FIPS and approved ANSI manuals can be ordered on DD Form 1425 from the U.S. Naval Publications and Forms Center, 5801 Labor Avenue, Philadelphia, Pennsylvania 19120.

1. True
2. False

2-39. ADPPRS data is to be reported in accordance with SECNAVINST 5231.1 series to COMNAVDAC, code 04.

1. True
2. False

Learning Objective: Identify the management strategies of personnel acquisition.

2-40. A DPI should be aware of which of the following management strategies?

1. The delineation of personnel responsibilities
2. The organizational structure of an ADP organization
3. The methods of personnel acquisition
4. Each of the above

2-41. The administration of naval personnel involves which of the following activities?

1. Classification
2. Evaluation
3. Separation
4. Each of the above

2-42. Which of the following is an objective of personnel administration in an ADP organization?

1. To ensure enough personnel assigned for a four-day work week
2. To ensure that extra personnel are assigned to the facility
3. To ensure maximum utilization of personnel assigned
4. To ensure that each person assigned has prior sea duty

2-43. Naval manpower and personnel administration are engineered to cope with which of the following problems at all organizational levels?

1. Hardware
2. Software
3. Security
4. Personnel

2-44. The responsibility for manpower management in the Navy begins with which of the following individuals?

1. The Chief of Naval Operations
2. The Secretary of the Navy
3. The Secretary for Manpower and Reserve
4. Commander, Naval Data Automation Command

2-45. Statistical forecasting, balancing, and manpower requirements relate to which of the following activity requirements?

1. Naval ships
2. Military billets
3. Automobiles
4. Civilian positions

2-46. The officer assigned as the Deputy Chief of Naval Operations for Manpower and Naval Reserve is also the

1. Chief of Naval Personnel
2. Chief of Naval Operations
3. Secretary of the Navy
4. Commandant of the Marine Corps

2-47. Which of the following instructions is the basis from which plans are developed to procure, train, and assign personnel?

1. SECNAVINST 1000.13 series
2. SECNAVINST 1301.1 series
3. OPNAVINST 1000.16 series
4. OPNAVINST 1301.1 series

2-48. The vital support of policy control and direction of the Navy Manpower Requirement System is provided by which of the following field components?

1. NAVMMACLANT
2. NAVMMACPAC
3. Both 1 and 2 above
4. CINCLANT

Learning Objective: Select the management strategies utilized to delineate personnel responsibilities.

2-49. Which of the following is the purpose of NAVMMACLANT/PAC?

1. To implement risk analysis studies for manpower
2. To apply work study and management engineering techniques to document and recommend the optimum use of manpower resources
3. To apply studies to data base management systems that apply to manpower resources
4. To store data base information on a Navy-wide spectrum to control information pertinent to the Privacy Act

2-50. The Department of Defense Planning, Programming, and Budgeting System operates on a cycle of what total number of months?

1. Eight
2. Twelve
3. Eighteen
4. Twenty-four

2-51. The President, the National Security Council, and the Department of Defense are involved in intelligence appraisals of any potential threat to the security of the Nation. Which of the following individuals and/or staffs issues the Defense Policy and Planning Guidance?

1. The National Security Council
2. The Secretary of Defense
3. The President
4. The Joint Chiefs of Staff

2-52. A Joint Force Memorandum is submitted to the Secretary of Defense by which of the following individuals and/or staffs?

1. The Joint Chiefs of Staff
2. The Vice President
3. The President
4. The National Security Council

2-53. The program objectives memorandum (POM) submitted to the Secretary of Defense is concentrated _____ (two), (four) fiscal years in advance of the current fiscal year and includes planned projections of forces programmed for _____ (six), (eight) fiscal years and manpower programmed for _____ (four), (five) fiscal years?

1. (a) four (b) six (c) five
2. (a) two (b) eight (c) five
3. (a) two (b) six (c) four
4. (a) four (b) eight (c) four

2-54. When do departments/agencies submit budget estimates to the SECDEF for the budget year?

1. During program decision process
2. When program decisions are finalized
3. Immediately prior to program decision finalization
4. When the agencies decide that it would be in their best interest

2-55. The budget year is usually the fiscal year in advance of the current fiscal year and is which of the following program years of the Five-year Defense Plan (FYDP)?

1. First
2. Second
3. Third
4. Fourth

2-56. Who promulgates the manpower authorizations (OPNAV FORM 1000/2)?

1. The Secretary of the Navy
2. The Secretary of Defense
3. The Chief of Naval Operations
4. The Chief of Naval Personnel

2-57. What is the single official statement of organizational manning and billet authorization?

1. OPNAVINST 1000.16 series
2. NAVDAC Pub 1
3. SECNAVINST 10265.1 series
4. OPNAV FORM 1000/2

2-58. Which of the following requirements is/are NOT subject to end-strength limitations?

1. Mobilization
2. Ship manning
3. Shore installation manning
4. Any ADP personnel needs

2-59. Changes to an activity's mission, tasks, or functions, which will require manpower changes, must be identified to the Chief of Naval Operations what minimum number of months prior to the beginning of the fiscal year in which the manpower change is required?

1. Six
2. Twelve
3. Eighteen
4. Twenty-four

Learning Objective: Identify the procedures required when requesting changes to manpower authorizations.

2-60. Billet changes requiring permanent change of station orders should be projected with an effective date a minimum of how many months from the date of approval?

1. Five
2. Six
3. Eight
4. Four

2-61. Who retains final decision authority on all billet change requests?

1. The Chief of Naval Personnel
2. The Chief of Naval Operations
3. The Secretary of the Navy
4. The Commander, Naval Data Automation Command

2-62. Billet change requests should be submitted a minimum of how many months prior to the effective date desired?

1. Six
2. Eight
3. Ten
4. Twelve

2-63. Requests for changes in manpower authorizations are forwarded via the chain of command to which of the following commands, bureaus, or offices?

1. The manpower claimant
2. The Bureau of Naval Material
3. The Office of the Secretary of the Navy
4. The Joint Chiefs of Staff

2-64. The manpower claimant forwards billet requests that are recommended for approval to what individual?

1. The Chief of Naval Personnel
2. The Chief of Naval Operations
3. The Chief of Naval Material
4. The Commander-in-Chief

2-65. Who makes recommendations to the Chief of Naval Operations about billet requirements for assigned activities and planned mobilization activities which do NOT exist in peacetime?

1. The activity's commanding officer
2. The activity's executive officer
3. The area's master chief petty officer
4. The manpower claimant

2-66. The OPNAV form used to request billet changes when submitting Manpower Authorization Requests is number

1. 1000/1A
2. 1000/2A
3. 1000/3A
4. 1000/4A

2-67. It is recommended that OPNAV Forms 1000/4A be submitted in which of the following manners?

1. Typed and letter perfect
2. Bold and legible, hand printed
3. Photographically reduced
4. Keypunched on cards

2-68. When a complete reorganization is NOT being requested, which of the following information should be entered on OPNAV Form 1000/4A?

1. Billets that are to be added
2. Billets that are to be changed
3. Billets that are to be deleted
4. All of the above

2-69. The original and what minimum number of copies of OPNAV Form 1000/4A should be submitted to the CNO?

1. One
2. Two
3. Three
4. Four

2-70. A short format of the manpower authorization form can be utilized for requesting which of the following changes?

1. A single additional billet
2. A paygrade change
3. A Navy enlisted classification code
4. A billet rate change

QUESTIONS 2-71 AND 2-72 ARE TO BE JUDGED TRUE OR FALSE.

2-71. The Manpower Authorization Short-Format Change Request may be used only by fleet and fleet staff units.

1. True
2. False

2-72. The Manpower Authorization Short-Format Change Request may be sent directly to the Chief of Naval Operations

1. True
2. False

Assignment 3

ADP Installation Characteristics and Risk Analysis

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 2-20 through 3-8

Learning Objective: Identify the personnel skills required to satisfy the ADP billet structure allowance.

3-1. At an ADP installation, the Navy assigns billets mostly by which of the following methods?

1. The size of the computer
2. The model of computer
3. The base location
4. The individual's NEC

3-2. Which of the following factors determine(s) the number of personnel required for an ADP facility?

1. The workload
2. The hours of operation
3. The mission of the facility
4. All of the above

3-3. Who is responsible for all data processing performed by an activity, including systems analysis, administration, programming, and operations?

1. The training technician
2. The senior systems analyst
3. The data processing manager
4. The data base administrator

3-4. Who coordinates data processing standards development and implementation?

1. The DP technical manager
2. The standards controller
3. The senior analyst
4. The operations supervisor

3-5. Who is responsible for professional technical development of personnel attached to the ADP facility?

1. The data base administrator
2. The tape librarian
3. The training technician
4. The senior programmer

QUESTIONS 3-6 THROUGH 3-12 ARE TO BE JUDGED TRUE OR FALSE.

3-6. A systems analysis supervisor is NEVER required to coordinate project control and approval.

1. True
2. False

3-7. The senior systems analyst is in direct liaison with the management and personnel of the user departments.

1. True
2. False

3-8. A systems analyst participates in the analysis of systems problems and the development of problem situations concerning software only.

1. True
2. False

3-9. A data base administrator supervisor approves all software and hardware changes affecting structure and administrative handling of the data base.

1. True
2. False

3-10. The senior data base administrator provides direction and control within command specifications for Data Base Management Systems and inherent schemas.

1. True
2. False

3-11. The programming supervisor provides technical and administrative direction to the systems analysis department.

1. True
2. False

3-12. The applications programmer participates in analysis liaison with the systems analyst.

1. True
2. False

3-13. Who supervises the operation of key-to-tape/disk equipment?

1. The senior programmer
2. The operations supervisor
3. The programming supervisor
4. The systems analyst

3-14. Who prepares the computer for program processing and is responsible for satisfactory completion of each scheduled computer operation?

1. The senior systems analyst
2. The tape librarian
3. The senior console operator
4. The maintenance programmer

3-15. Who directs the control and coordination of all operational facilities through supervising library activities, production control procedures, and operating standards?

1. The operations supervisor
2. The key-to-tape/disk supervisor
3. The operations control supervisor
4. The programming supervisor

3-16. Who controls foreign recording media?

1. The tape librarian
2. The analyst
3. The operator
4. The programmer

Learning Objective: Describe the characteristics of ADP installations in the Navy.

3-17. At which of the following types of commands should a DP expect the most cross-training?

1. A communications station
2. A ship
3. A supply facility
4. A naval air station

3-18. For an activity to have a DPID, it must have at least (a) (one), (two) central processing unit(s) and (b) (one), (two) computer operator(s)?

1. (a) one (b) two
2. (a) one (b) one
3. (a) two (b) one
4. (a) two (b) two

3-19. When an activity has a data processing programming support department (DPPSD), it must have an organizational element with which of the following primary functions?

1. To design application software/computer programs
2. To develop application software/computer programs
3. To maintain application software/computer programs
4. Each of the above

3-20. For an ADP activity to have a DPPSD, it should have what minimum number of programmers/analysts/specialists?

1. Five
2. Six
3. Three
4. Four

3-21. For an installation to have a technical support department (TSD), the activity must have an organizational element that provides which of the following primary functions?

1. Specialized technical support
2. Generalized technical support
3. Developmental technical support
4. Research technical support

3-22. When planning for incoming hardware at a new installation, the planner's primary concern(s) should be for

1. space only
2. arrangement only
3. environment only
4. space, arrangement, and environment

3-23. Each NARDAC is organized under a standard structure patterned after which of the following commands?

1. CINCLANT
2. CINCPAC
3. NAVDAC
4. NAVAIR

Learning Objective: Select the risk analysis procedures as the basis for development of a security policy for a DP facility.

QUESTIONS 3-24 AND 3-25 ARE TO BE JUDGED TRUE OR FALSE.

3-24. The physical security program for a highly classified defense command should be comparable with the physical security program of an unclassified, nontactical command.

1. True
2. False

3-25. A physical security program for an ADP facility in Florida would require as much emphasis on earthquake protection as would an ADP facility in California.

1. True
2. False

3-26. The impact of a given threat to an ADP facility may depend on which of the following factors?

1. The perceived importance of the facility to activists or subversives
2. The local environment
3. The geographic location of the facility
4. Each of the above

3-27. Which of the following is a threat to an ADP facility?

1. ADP hardware failures
2. Accidents causing the nonavailability of key personnel
3. Tampering with input, programs, and data
4. Each of the above

3-28. It is recommended that the ADP facility upper management begin development of the physical security program with a/an

1. intensive training program
2. inventory of equipments
3. risk analysis
4. survey of data integrity

3-29. A quantitative risk produces which of the following benefits?

1. Long-range planners receive guidance on personnel requirements
2. The security program objectives directly relate to the mission of the command
3. Criteria are generated for designing and evaluation contingency plans
4. Both 2 and 3 above

3-30. The first step to be considered when the risk analysis is prepared is to

1. estimate the potential losses to which the ADP facility is exposed
2. evaluate the threats to the ADP facility
3. develop an estimate of annual loss expectancy
4. review the security program objectives

3-31. Which of the following is/are the objective(s) of the loss potential estimate?

1. Identify critical aspects of the ADP facility operation
2. Place a monetary value on the loss estimate
3. Both 1 and 2 above
4. Determine data replacement requirements

IN ANSWERING QUESTIONS 3-32 THROUGH 3-35, SELECT THE LOSS POTENTIAL IN COLUMN A THAT IS APPLICABLE TO THE SITUATION IN COLUMN B. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. LOSS POTENTIAL	B. SITUATION
3-32.	Cost to replace assets	1. Loss of program files
3-33.	Cost to reconstruct files	2. Indirect theft of assets
3-34.	Value of assets stolen before loss is detected	3. Theft of information
3-35.	Security compromise	4. Theft of tangible assets

3-36. The DP technical manager should call on which of the following personnel to assist in making loss estimates?

1. Supervisors
2. Users
3. Contractors
4. All of the above

IN ANSWERING QUESTION 3-37, REFER TO FIGURE 3-1 IN TEXT.

3-37. The task receiving a MANPOWER COST ESTIMATE of 1 week, received a DELAYED PROCESSING IMPACT estimate considered to be what relative value?

1. Very Low
2. Low
3. Moderate
4. Extreme

3-38. After a preliminary screening to identify the critical tasks, the DP technical manager should do which of the following tasks next?

1. Determine the scope of the critical tasks
2. Quantify loss potential with the help of user representatives
3. Determine the back-up system requirements for the critical tasks
4. All of the above

3-39. The second step to be considered when preparing the risk analysis is to

1. evaluate the threats to the ADP facility
2. review the security program objectives
3. estimate the potential losses to which the ADP facility is exposed
4. develop an estimate of annual loss expectancy

3-40. When estimating the occurrence probability for each type of threat, the DP technical manager should use which of the following resources?

1. General information
2. Common sense
3. Higher authority instructions/ manuals
4. All of the above

QUESTION 3-41 IS TO BE JUDGED TRUE OR FALSE

3-41. For security reasons, the overall risk analysis should be conducted by the DP technical manager without the participation of other ADP facility personnel.

1. True
2. False

3-42. The third step to be considered when preparing the risk analysis is to

1. review the security program objectives
2. estimate the potential losses to which the ADP facility is exposed
3. develop an estimate of annual loss expectancy
4. evaluate the threats to the ADP facility

3-43. Which of the following is the purpose of an annual loss expectancy?

1. To determine which personnel will be responsible for each security measure
2. To pinpoint the significant threats as a guide to selecting security measures
3. To determine the amount of money to spend on each security measure
4. Both 2 and 3 above

3-44. Fire, flood, and sabotage, in varying degrees, result in which of the following losses?

1. Physical destruction
2. Delayed processing
3. Both 1 and 2 above
4. Theft of information

QUESTION 3-45 IS TO BE JUDGED TRUE OR FALSE.

3-45. In each case where there can be significant loss, the loss potential is multiplied by the probability of occurrence of the threat to generate an annual estimate of loss.

1. True
2. False

Learning Objective: Select the appropriate security measures to reduce exposure to losses in an ADP facility.

IN ANSWERING QUESTIONS 3-46 THROUGH 3-49, SELECT THE SPECIFIC RESPONSE IN COLUMN A THAT IS APPROPRIATE FOR THE RESPONSE FORM IN COLUMN B. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

A. SPECIFIC RESPONSE	B. RESPONSE FORM
3-46. Prepare a backup system for off-site operation	1. Alter the environment
3-47. Provide intrusion detectors, military guards, and special door locks	2. Improve procedures
3-48. Implement more rigorous standards for programming and software testing	3. Establish contingency plans
3-49. Relocate the ADP facility	4. Erect barriers

IN ANSWERING QUESTION 3-50, REFER TO FIGURE 3-3 IN TEXT.

3-50. Which remedial measure is effective against all but one threat?

1. Intrusion detector
2. Roving guard patrol
3. Back-up plan
4. Loss control team

3-51. Which of the following is one possible way to select a remedial measure to minimize a threat?

1. Begin with the threat having the largest annual loss potential
2. Begin with the remedial measures for which the annual cost is more than the expected reduction in annual loss
3. Begin with only those measures for which the cost can be estimated precisely
4. Begin with only those remedial measures that would not cause a loss reduction in the same area

REMEDIAL MEASURES	THREATS											
	A			B			C			D		
1	3	1	2	13	3	10	4	3	1	16	14	2
2	2	1	1	13	3	10	3	3	0	10	9	1
3	1	3	-2	7	0	7	3	2	1	9	2	7
4	4	4	0	4	2	2	4	2	2	8	3	5

FIGURE 3-A--THREAT MATRIX

IN ANSWERING QUESTIONS 3-52 THROUGH 3-54, REFER TO FIGURE 3-A.

3-52. Which remedial measure is the most effective on threat A?

1. 1
2. 2
3. 3
4. 4

3-53. Which remedial measure is the most totally effective on threats B, C, and D?

1. 1
2. 2
3. 3
4. 4

3-54. Which remedial measure is the most totally effective on all threats?

1. 1
2. 2
3. 3
4. 4

3-55. In producing a threat matrix, which of the following factors is/are established and documented?

1. The annual loss potential of critical tasks
2. The annual cost and loss reduction from remedial measures
3. Both 1 and 2 above
4. The annual percentage of non-essential maintenance performed

Learning Objective: Identify the various steps in implementing an ADP security program.

3-56. When an ADP security program is planned, which of the following is the suggested sequence of steps?

1. Conduct preliminary planning, implement urgent quick fix, and perform preliminary risk analysis
2. Establish an ADP security team, identify major problem areas, and document a detailed risk analysis
3. Implement urgent quick fix, justify cost and document action plans, and document a deteiled risk analysis
4. Conduct preliminary planning, document a detailed risk analysis, and implement urgent quick fix

3-57. After the detailed risk analysis is approved, the next step in implementing a security program is to justify and document which of the following plans?

1. Contingency plans
2. Training and indoctrination plans
3. Test and audit plans
4. All of the above

IN QUESTIONS 3-58 THROUGH 3-61, MATCH THE DOCUMENT IN COLUMN A WITH THE DOCUMENTATION ACTIVITY IN COLUMN B. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. DOCUMENT	B. DOCUMENTATION ACTIVITY
3-58.	Security policy statement	1. Reflects security objectives and requirements
3-59.	Security handbook	2. Provides general guidance and assigns responsibilities
3-60.	Command Standards	3. Indoctrinates staff in security program requirements
3-61.	Command Instructions	4. Describes in detail the security program and procedures

QUESTION 3-62 IS TO BE JUDGED TRUE OR FALSE.

3-62. The action plans for an ADP security program must be documented as completely separate items.

1. True
2. False

IN QUESTIONS 3-63 THROUGH 3-65, MATCH THE INSTRUCTIONS AND MANUALS IN COLUMN A WITH THE CONTENT IN COLUMN B. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. INSTRUCTIONS AND MANUALS	B. CONTENT
3-63.	OPNAVINST 5239.1 series with enclosures	1. Department of the Navy Information Security Program regulations
3-64.	OPNAVINST 5510.1 series	2. Guide for Security Equipment
3-65.	Office of Naval Intelligence	3. Department of the Navy security program for Automatic Data Processing systems

Assignment 4

Fire Safety and Contingency Plans

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 3-8 through 3-20

Learning Objective: Select the methods of fire safety, detection, and extinguishment used in an ADP facility.

4-1. In minimizing an ADP building to fire damage, which of the following factors should be considered?

1. Building contractors
2. Building design
3. Building location
4. Both 2 and 3 above

4-2. Which of the following is/are (a) fire safety element(s) that should be included in an ADP physical security program?

1. Measures to ensure prompt detection of and response to a fire emergency
2. Provision for quick human intervention and adequate means to extinguish fires
3. Provision of adequate means and personnel to limit damage and effect prompt recovery
4. All of the above

4-3. Generally speaking, the degree of hazard associated with a given occupancy (material) depends on the

1. amount of combustible material
2. weight of the material
3. exposed surface area of the material
4. package in which the material is stored

IN ANSWERING QUESTION 4-4, REFER TO FIGURE 3-5 IN TEXT.

4-4. Which of the five basic types of construction is the least flammable?

1. Noncombustible
2. Heavy timber
3. Fire resistant
4. Ordinary construction

4-5. Which of the following is/are (a) fire safety factor(s) to consider when the building for an ADP facility is designed?

1. Adequate ventilation
2. Fire walls
3. Heat resistant lights
4. Storm windows

QUESTIONS 4-6 AND 4-7 ARE TO BE JUDGED TRUE OR FALSE.

4-6. It is recommended that the assistance of a qualified fire protection engineer or local base fire personnel be sought in evaluating the inherent fire safety of the ADP facility.

1. True
2. False

4-7. The lack of sprinkler protection was NOT a factor in fighting the July 1973 fire at the U.S. Military Personnel Records Center in Overland, Missouri.

1. True
2. False

4-8. The inherent fire safety of a building can be rendered ineffective because of which of the following hazards?

1. Substandard electric wiring
2. Fire doors propped open
3. Undue accumulation of debris or trash
4. Each of the above

4-9. Experience in fire fighting has shown that the major factor in limiting fire damage is

1. experienced fire fighters
2. early detection of fires
3. quick response time to alarms by fire fighters
4. multiple fire extinguishers

4-10. During the third stage of the fire, fire fighting becomes increasingly difficult and often people CANNOT remain at the fire site because of which of the following reasons?

1. High temperatures
2. Large volumes of smoke
3. Toxic gases
4. All of the above

4-11. Prompt fire detection is best accomplished through the use of

1. smoke detectors
2. heat detectors
3. gas detectors
4. flame detectors

4-12. Which, if any, of the following factors should NOT be considered when detectors are installed?

1. The direction and velocity of air flow
2. The presence of areas with stagnant air
3. The location of equipment and other potential fire sites
4. None of the above

4-13. Which of the following indications is/are included on the detection control panel?

1. Indicates the power supply status of each detector
2. Indicates which detector has alarmed
3. Indicates the location of the detector which has alarmed
4. All of the above

4-14. To assure that someone will always be alerted to a fire, which of the following additional alarm locations should be provided?

1. Computer room
2. Personnel office
3. Commanding Officer's office
4. All of the above

QUESTIONS 4-15 AND 4-16 ARE TO BE JUDGED TRUE OR FALSE.

4-15. Reducing the sensitivity in smoke detectors to eliminate nuisance alarms may delay the detection of an actual fire.

1. True
2. False

4-16. In addition to alerting personnel to the presence of a fire, the detection equipment can be used to control the air conditioning system.

1. True
2. False

4-17. In an actual fire situation, the air handling equipment should be shut down automatically to avoid

1. excessive energy consumption
2. fanning the flames
3. strain on the air handling equipment
4. excessive filter wear

4-18. When fire detection systems are interconnected with air handling equipment, a preferred technique is to cause the system to take which of the following measures?

1. Lower the thermostat
2. Exhaust the smoke
3. Both 1 and 2 above
4. Recirculate the smoke

4-19. What is the minimum temperature required to activate an automatic sprinkler system?

1. 110°
2. 125°
3. 135°
4. 145°

4-20. To ensure the effectiveness of portable fire extinguishers, which of the following measures should be observed?

1. Extinguishers should be marked for rapid identification
2. Extinguishers should be placed in corners
3. Extinguishers should have inspection tags
4. All of the above

QUESTIONS 4-21 AND 4-22 ARE TO BE JUDGED TRUE OR FALSE.

4-21. Small commands, in general, need military personnel who are knowledgeable and trained in fire safety more so than large commands.

1. True
2. False

4-22. Key personnel who extingish fires must know how to turn in an alarm, which type of extinguisher to use for which type of fire, and how to use it.

1. True
2. False

Learning Objective: Select the problems that may occur to the electric power utility which ADP facilities depend on.

QUESTION 4-23 IS TO BE JUDGED TRUE OR FALSE.

4-23. A risk analysis establishes the possible effects of breakdowns, sabotage, vandalism, fire, and flooding on an ADP facility.

1. True
2. False

4-24. The filtering and regulation of line voltage CANNOT be expected to eliminate voltage variations beyond a reasonable range. What is the minimum-fluctuation in line voltage which will cause excessive fluctuation in the d.c. voltage applied to the hardward?

1. 90 percent or less of nominal for more than 7 milliseconds
2. 90 percent or less of nominal for more than 6 milliseconds
3. 90 percent or less of nominal for more than 5 milliseconds
4. 90 percent or less of nominal for more than 4 milliseconds

4-25. Power fluctuations in line voltage cause unpredictable results on which of the following ADP components?

1. Hardware
2. Logic
3. Data transfer
4. All of the above

4-26. The effects of internal power fluctuations can be minimized in an ADP facility by

1. isolating the ADP hardware from other facility loads
2. grounding the CPU
3. wiring all components in parallel
4. wiring each component with a circuit breaker

4-27. When connecting the ADP facility to more than one utility feeder, the technique has more protection value when the feeders are connected in what manner?

1. To the same junction box
2. From the same utility pole
3. To different power substations
4. To different meters

4-28. An uninterrupted power supply (UPS) consists of a solid-state rectifier which performs which of the following functions?

1. Synthesizes alternating current
2. Keeps batteries charged
3. Drives a solid-state invertor
4. Both 2 and 3 above

4-29. The UPS battery supply can support a facility load for a maximum of

1. 25 minutes
2. 35 minutes
3. 45 minutes
4. 55 minutes

4-30. The control circuitry for a static transfer switch (installed between the UPS and the computer) performs which of the following functions?

1. Senses variations in frequency
2. Switches the load to the prime source without causing a noticeable transient
3. Senses an overcurrent condition
4. Both 2 and 3 above

4-31. Which of the following benefits is/are derived from using multiple, independent UPS units?

1. Each unit can be switched off-line if it fails
2. Power consumption is lowered
3. The metering of component power consumption is facilitated
4. All of the above

4-32. Which of the following measures should be taken if the risk analysis has shown a major loss from power outages lasting 30 to 45 minutes or beyond?

1. Add more multiple, independent UPS units
2. Cut back on operations
3. Install an onsite generator
4. Both 2 and 3 above

QUESTIONS 4-33 AND 4-34 ARE TO BE JUDGED TRUE OR FALSE.

4-33. After the external power has failed, the UPS switches over to the generator when the control unit starts the prime mover.

1. True
2. False

4-34. In addition to the UPS load, the onsite generator must be large enough to support other essential loads, such as air conditioning or minimum lighting.

1. True
2. False

Learning Objective: Select the methods appropriate to ensure physical protection for an ADP facility.

4-35. Which of the following processes is/are involved in providing physical protection for an ADP facility?

1. Permitting access to authorized persons
2. Denying access to unauthorized persons
3. Both 1 and 2 above
4. Minimizing risks from natural disasters

4-36. Which, if any, of the following contingency plans for dealing with classified material should NOT be considered in emergencies?

1. Protection of material
2. Removal of material
3. Destruction of material
4. None of the above

4-37. In an emergency, the placement of a perimeter guard force around the affected area provides protection in which of the following ways?

1. Provides external contact when communications are lost
2. Prevents the removal of classified material
3. Reduces the risk of casualties
4. Both 2 and 3 above

QUESTIONS 4-38 AND 4-39 ARE TO BE JUDGED TRUE OR FALSE.

4-38. The physical security requirements for the computer area should be consistent with the classification of the information being handled.

1. True
2. False

4-39. When two or more computer systems are located in the same controlled area, direct personnel access to all systems should be provided.

1. True
2. False

4-40. Fences installed for boundary protection should be (a) what minimum height with (b) what minimum number of strands of barbed wire?

1. (a) 7 (b) two
2. (a) 8 (b) two
3. (a) 8 (b) three
4. (a) 9 (b) two

4-41. Penetration sensors mounted on fences and gates should provide which of the following alarms when tripped?

1. External and internal sound alarm
2. External lights
3. Internal sound alarm
4. Both 2 and 3 above

4-42. Tests have shown that electromagnetic or acoustic emanations from ADP hardware may be intercepted up to a maximum of

1. 100 meters away
2. 200 meters away
3. 300 meters away
4. 400 meters away

4-43. If the DP technical manager plans to take measures to control compromising emanations, those measures are subject to approval under the provisions of which of the following DOD Directives?

1. 5200-19
2. S-5200-19
3. S-5200.20
4. S-5200-22

4-44. The Joint-Services Interior Intrusion Detection System (J-SIIDS) does NOT provide internal tamper switches in which of the following components?

1. Duress sensors
2. Monitors
3. Control unit
4. Each of the above

IN ANSWERING QUESTION 4-45, REFER TO FIGURE 3-10 IN TEXT.

4-45. The control unit contains which of the following components?

1. Access/test/secure switch
2. Signal module
3. Data receiver
4. Both 2 and 3 above

4-46. The monitoring and display equipment normally is located in an area having which of the following qualities?

1. A protected area
2. An area where monitoring personnel are on duty 24 hours a day
3. An area that has no windows
4. All of the above

4-47. The alarm monitor module gives which of the following indications?

1. Audible indication of alarm conditions
2. Audible indication of status changes
3. Visual indication of alarm changes
4. All of the above

QUESTIONS 4-48 THROUGH 4-51 ARE TO BE JUDGED TRUE OR FALSE.

4-48. The "Guide for Security Equipment," ONI-CS-63-1-76, is published by the Office of Naval Intelligence and describes all J-SIIDS components and the use of each.

1. True
2. False

4-49. Remote terminal area requirements are based upon the lowest classified and least restrictive category of material which will be accessed through the terminal under system constraints.

1. True
2. False

4-50. Security measures for terminals operated by personnel NOT responsible for the overall operation of the ADP system should be agreed to and implemented before the terminal is connected to the ADP system.

1. True
2. False

4-51. Though a terminal is NOT cleared for classified material, the terminal may NOT be disconnected from the ADP system when the system contains classified information.

1. True
2. False

4-52. The second step of an annual security survey of an ADP facility is to

1. define and tabulate areas within the facility for control purposes
2. recommend improvements to upper management
3. identify areas where remedial measures are needed
4. evaluate all potential threats to the ADP facility

4-53. The annual physical security survey of the ADP facility need NOT include which of the following common areas?

1. Loading dock
2. ADP facility reception area
3. Air conditioning spaces
4. Restroom area

4-54. In conducting the annual physical security survey, the DP technical manager should begin at the

1. roof
2. top floor
3. perimeter
4. basement

4-55. When surveying the property line of an ADP facility, the DP technical manager should determine which of the following facts?

1. The type of fence installed
2. The contractor who installed the fence
3. The installation date of the fence
4. All of the above

4-56. When surveying the perimeter of the facility, the DP technical manager should NOT check which, if any, of the following accessways?

1. All doors and windows
2. All fire escapes
3. Other entrances such as vents
4. None of the above

4-57. When surveying the internal security of a facility, the DP technical manager should follow which of the following guidelines?

1. Begin the survey on the roof
2. Determine where alarms annunciate
3. Finish the survey in the restroom area
4. All of the above

4-58. Which of the following questions need NOT be included in the physical security survey?

1. Is the present equipment outdated?
2. Is the alarm system inspected and tested occasionally to ensure operation?
3. What kind of sound does the alarm annunciate?
4. How many zones of protection are within the protected building?

4-59. Which, if any, of the following records should NOT be kept on alarm signals?

1. Time and date of alarm
2. Location of alarm
3. Cause of alarm
4. None of the above

Learning Objective: Identify the procedures for developing and implementing contingency plans for an ADP facility.

QUESTIONS 4-60 THROUGH 4-62 ARE TO BE JUDGED TRUE OR FALSE.

4-60. The operation plans for an ADP facility assume normal working conditions.

1. True
2. False

4-61. The DP technical manager should recognize that preventive measures will maintain the normal working conditions assumed by the operation plans.

1. True
2. False

4-62. The text refers to a COOP security program. The acronym COOP stands for cooperation.

1. True
2. False

4-63. Contingency plans for an ADP facility include which of the following types of plans?

1. Recovery
2. Backup operations
3. Emergency response
4. Each of the above

IN ANSWERING QUESTION 4-64, REFER TO FIGURE 3-11 IN TEXT.

4-64. The User Representatives should be involved in which of the following tasks?

1. Emergency response plans
2. Failure mode analysis
3. Selection of backup modes
4. All of the above

QUESTIONS 4-65 THROUGH 4-67 ARE TO BE JUDGED TRUE OR FALSE.

4-65. The term emergency response planning refers to steps taken immediately before an emergency occurs.

1. True
2. False

4-66. The risk analysis should be reviewed by the DP technical manager to identify emergency conditions which have particular implications for ADP operations.

1. True
2. False

4-67. The Loss Control Plan should be implemented as part of COOP.

1. True
2. False

4-68. Which of the following guidelines should a DP technical manager use to develop emergency measures?

1. Notify online users of the service interruption
2. Cover ADP hardware with water proof material and leave the power on
3. Ensure that the air-conditioning equipment is on
4. All of the above

4-69. All personnel should be instructed to take which of the following security measures if an evacuation of work areas is ordered?

1. Secure unclassified materials in desks or file cabinets
2. Turn off equipment but leave room lights on
3. Close the doors as areas are evacuated but leave the doors unlocked
4. All of the above

4-70. To assure that all safety requirements of the ADP facility are satisfied, the DP technical manager and the operations division officer should periodically review the protective plans at what frequency?

1. Once a month
2. Four times a year
3. Twice a year
4. Once a year

4-71. The emergency response plan for a fire emergency should include which of the following steps?

1. Assess life-safety hazard
2. Initiate loss control procedures
3. Both 1 and 2 above
4. Contact insurance company

4-72. Backup operations may take place onsite following which of the following conditions?

1. A partial loss of capability
2. Major damage or destruction
3. Both 1 and 2 above

4-73. When backup operations are considered, quite often ADP management will find which of the following situations?

1. An exact replica of the onsite ADP system is not available for backup
2. The time available per day is less than what is needed to complete all assigned tasks
3. Both 1 and 2 above
4. Backup operations are not needed

4-74. For the purpose of making back-up resources available, which of the following tasks can be set aside?

1. Long-range planning
2. Program development
3. Long cycle processing
4. Each of the above

4-75. When considering back-up alternatives, which of the following substitute procedures may be implemented during an emergency?

1. A punched card input could be used for a failed telephone input
2. Batch processing could be substituted for online processing
3. Print tapes could be carried to a backup facility for offline printing
4. Both 2 and 3 above

Assignment 5

Physical Security and Privacy Act Requirements

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 3-20 through 3-33

QUESTIONS 5-1 AND 5-2 ARE TO BE JUDGED TRUE OR FALSE.

5-1. Where compatible hardware is not available, it may be feasible to maintain a second software package as a backup system which is functionally identical to the regular package but technically compatible with the offsite ADP hardware that is available for backup use.

1. True
2. False

5-2. To stretch available backup resources, it might be feasible to halve the cycle time for a task, that is, run a daily task twice a day.

1. True
2. False

5-3. When evaluating alternate backup modes and offsite facilities, the DP technical manager should consider which of the following factors?

1. Transportation of personnel with needed supplies and materials
2. Maintenance personnel at the offsite location
3. Overtime cost factor for civil service personnel
4. All of the above

5-4. When developing the optimum backup plan, it is wise to form several backup plans, one of which has which of the following characteristics?

1. Extends beyond the cause of delay
2. Lasts at least half the time required to reconstruct the facility
3. Includes one or more operating periods between minimum duration and worst case
4. Includes each minor partial failure

IN QUESTIONS 5-5 THROUGH 5-8, MATCH THE BACKUP PLAN AREAS WITH THE CONTENT DESCRIPTION.

A. BACKUP PLAN AREA	B. CONTENT DESCRIPTION
5-5. Performance specifications	1. Administrative information about the terms of backup use
5-6. User Instructions	2. Special personnel assignments, use of special messengers, temporary employment
5-7. Computer system specifications	3. Requirements of different input forms
5-8. Administrative information	4. Specific ways in which performance of each task departs from normal

5-9. The process of recovery will be carried out more effectively and economically if

1. personnel other than ADP staff handle recovery
2. the ADP staff handles recovery
3. the ADP staff and users handle recovery
4. the users handle recovery

5-10. Which of the following tasks require completion before recovery from total destruction is achieved?

1. Facility modifications
2. Hardware procurement
3. Hardware, equipment, and materials verification
4. All of the above

IN ANSWERING QUESTION 5-11, REFER TO FIGURE 3-12 IN TEXT.

5-11. Before the electric power and air conditioning can be installed, which of the following reconstruction steps must be completed?

1. Procure ADP hardware
2. Procure needed floor space
3. Procure supplies needed for check out
4. All of the above

QUESTIONS 5-12 AND 5-13 ARE TO BE JUDGED TRUE OR FALSE.

5-12. The availability of needed back-up files may be tested by repeating a particular task using onsite hardware but drawing everything else from the offsite location.

1. True
2. False

5-13. Compatibility with the offsite facility needs to be verified only one time.

1. True
2. False

Learning Objective: Identify the procedures to be followed when conducting a physical security audit of an ADP facility.

5-14. Which of the following is/are (a) standard(s) for an ADP facility audit?

1. Is independent and objective
2. Examines the information system and its use
3. Both 1 and 2 above
4. Should be the first element in a physical security program

5-15. The characteristic of an audit being independent and objective implies that the audit

1. replaces normal management inspections
2. is a substitute for management reporting systems
3. complements normal management inspections
4. is a part of normal management visibility

5-16. An audit can be expected to accomplish which of the following tasks?

1. It evaluates security controls for the ADP facility
2. It provides each level of management an opportunity to maintain its current security program
3. It provides the impetus to keep workers and management complacent
4. Each of the above

5-17. In determining the frequency of internal audits, the ADP technical manager should consider which of the following factors?

1. The frequency of external audits
2. The rate of change of the ADP system
3. The results of previous audits
4. All of the above

QUESTIONS 5-18 THROUGH 5-21 ARE TO BE JUDGED TRUE OR FALSE.

5-18. One of the main principles of audit team selection is that members should be responsible for ADP operations.

1. True
2. False

5-19. The audit should be conducted by some department or facility within the control of the DP technical manager.

1. True
2. False

5-20. The character of each prospective audit team member is not a consideration for team selection.

1. True
2. False

5-21. The leader of the audit team must be able to organize the efforts, prepare a good written report, and communicate findings effectively.

1. True
2. False

5-22. Which, if any, of the following characteristics is/are NOT desired for audit board members?

1. Inquisitiveness
2. A probing nature
3. Attention to detail
4. None of the above

5-23. The group of people who have the most to gain from an ADP facility audit are the

1. members of the audit team
2. users of the facility
3. members of the security force
4. programmers in the facility

5-24. One of the prime requirements of the audit team is that it consist of people who are

1. objective
2. subjective
3. employed in the facility
4. supervisors

5-25. Which of the following is/are (a) characteristic(s) of a comprehensive audit plan?

1. It is action-oriented
2. It lists actions to be performed
3. It is tailored to the particular installation
4. Each of the above

5-26. The third step in developing a comprehensive audit plan is to

1. review documents to determine the specified security operating procedures
2. examine the security policy and extract pertinent objectives
3. review the risk analysis plan
4. examine the ADP facility organization chart and job descriptions

5-27. Which of the following questions should be considered when formulating the audit program?

1. What measures are tested most frequently in day-to-day operations?
2. What are the critical issues with regard to security?
3. What audit activities produce the minimum results with the most effort?
4. Each of the above

5-28. It is considered advantageous to test fire detection sensors under surprise conditions because of which of the following reasons?

1. It tests the response to alarms
2. It tests the reaction of the fire party
3. It tests the effectiveness of evacuation plans
4. Each of the above

5-29. Which of the following is/are (an) advantage(s) gained from using a scheduled audit?

1. It motivates cleaning up loose ends
2. It reveals personnel complacency
3. It provides a test of response to fire
4. All of the above

5-30. A surprise audit should be approved by which of the following personnel?

1. The Officer in Charge of the ADP facility
2. The Commanding Officer of the command in charge of the ADP facility
3. Both 1 and 2 above
4. The Commander of the District in which the ADP facility is located

5-31. In conducting an audit, the first step normally is to

1. scrutinize the ADP facility records
2. interview the ADP personnel
3. survey the ADP hardware capabilities of the facility

5-32. When conducting an interview, the interviewer should follow which of the following guidelines?

1. Strive to be open in dealing with the interviewees
2. Avoid allusions to private information
3. Avoid obscure references to other people
4. All of the above

QUESTIONS 5-33 THROUGH 5-35 ARE TO BE JUDGED TRUE OR FALSE.

5-33. Any answer the interviewee provides that appears to be evasive or defensive should be probed in some detail.

1. True
2. False

5-34. If the interviewer decides to tape-record the interview, it is recommended NOT to inform the interviewee of the taping.

1. True
2. False

5-35. It is possible to test the adequacy of programmed controls and data authorization by submitting jobs that attempt to bypass these controls.

1. True
2. False

5-36. Most security audits include testing which of the following activities at ADP facilities?

1. Fire detection
2. Facility evacuation
3. Disaster recovery
4. Each of the above

5-37. What is the requirement for how often the audit team should convene to review progress and compare notes?

1. At the end of each day's activity
2. At the end of each week's activity
3. Every two weeks
4. Every three weeks

5-38. After the completion of the audit, when should the written report be prepared?

1. When requested by the supervisor of the ADP facility being audited
2. When requested by the commanding officer of the ADP installation where the ADP facility is located
3. After an extended period of time so that team members can reflect on the audit process
4. Immediately after the audit is completed

5-39. The person responsible for implementing the recommendations received from an audit is the

1. ADP technical manager
2. facility officer in charge
3. commanding officer of the command
4. district commander

5-40. The best approach in assigning responsibilities for corrective action is to summarize each major deficiency on a control sheet outlining which of the following areas?

1. Requirements and problem definition
2. Action taken or required
3. Responsibility and follow-up
4. All of the above

QUESTIONS 5-41 AND 5-42 ARE TO BE JUDGED TRUE OR FALSE.

5-41. Semiannual reports are recommended for any audit control items still open.

1. True
2. False

5-42. The emphasis of the audit should always be negative so that an objective evaluation is possible.

1. True
2. False

Learning Objective: Identify the procedures that the Privacy Act of 1974 requires of ADP facilities handling personnel data.

5-43. Which of the following instructions provides guidelines for implementing security safeguards required to implement the Privacy Act of 1974?

1. SECNAVINST 5221.5
2. SECNAVINST 5239.1
3. OPNAVINST 5510.1
4. OPNAVINST 5510.131

QUESTIONS 5-44 THROUGH 5-47 ARE TO BE JUDGED TRUE OR FALSE.

5-44. The identity of an individual requesting personal record information need not be confirmed before the information is released.

1. True
2. False

5-45. An individual must be granted access to their personal files on request.

1. True
2. False

5-46. Any request from an individual concerning the amendment of any record or information pertaining to the individual must be granted.

1. True
2. False

5-47. Rules of conduct are established for the guidance of Department of the Navy personnel who are subject to criminal penalties for noncompliance with the Privacy Act.

1. True
2. False

5-48. Which of the following subsections of the Privacy Act (title 5, section 552a) requires the use of safeguards to ensure the confidentiality and security of records?

1. Subsection (b)
2. Subsection (e) (5)
3. Subsection (e) (10)
4. Subsection (f)

IN QUESTIONS 5-49 THROUGH 5-52, SELECT FROM COLUMN B THE DEFINITION OF THE TERM IN COLUMN A.

5-49.	Data integrity	1. The protection of data from unauthorized modification, destruction, or disclosure
5-50.	Information Management Practices	2. Hardware and software techniques for controlling the processing of and access to data and other assets
5-51.	Data Security	3. Procedures for collecting, validating, processing, controlling, and distributing data
5-52.	Computer System Network Security Controls	4. When data agrees with the source from which it is derived

---

QUESTIONS 5-53 THROUGH 5-56 ARE TO BE JUDGED TRUE OR FALSE

5-53. A data security risk assignment provides a basis for deciding whether fewer safeguards are needed for data.

1. True
2. False

5-54. The seriousness of a risk depends on both the potential impact of the event and its probability of occurrence.

1. True
2. False

5-55. The participants on the risk assessment team should include experienced representatives from the facility responsible for managing ADP operations.

1. True
2. False

5-56. Experience indicates that the most commonly encountered security risks are usually subversive attempts.

1. True
2. False

5-57. Personal data can be retrieved from waste paper baskets, magnetic tapes, or discarded files as a result of

1. mistaken processing of data
2. careless disposal of data
3. program errors
4. improper data dissemination

5-58. Data may be misrouted, mislabeled, or it may contain unexpected personal information as a result of

1. improper data dissemination
2. input errors
3. mistaken processing of data
4. program errors

5-59. Which of the following risks should be considered if there are persons working on the system who have limited access to the files?

1. Open system access
2. Dial-in access
3. Open access during abnormal circumstances
4. Each of the above

QUESTIONS 5-60 AND 5-61 ARE TO BE JUDGED TRUE OR FALSE.

5-60. Physical destruction or disabling of the ADP system is normally a primary risk to privacy.

1. True
2. False

5-61. All computer systems presently in use are vulnerable to deliberate penetrations which can bypass security controls.

1. True
2. False

5-62. System personnel or the system software can be mislead into performing an operation that appears normal but actually results in unauthorized access through a method called

1. eavesdropping
2. misidentified access
3. spoofing-actions
4. subverting programs

5-63. Communications lines can be "monitored" by unauthorized terminals to obtain or modify information or to gain unauthorized access to an ADP system and is called

1. subverting programs
2. misidentified access
3. spoofing-actions
4. eavesdropping

5-64. Information management practices include which of the following activities?

1. Data collection, validation, and transformation
2. Information processing or handling
3. Information control, display, and presentation
4. All of the above

5-65. Which of the following practices is/are suggested for the handling of personal data?

1. Label recording media which contain data of local personnel only
2. Carefully control products of intermediate processing steps
3. Maintain an up-to-date hard copy authorization list of all individuals allowed to access personal data
4. Both 2 and 3 above

5-66. Which of the following practices is/are suggested for the maintenance of personal records?

1. Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility
2. Maintain logbooks for terminals that are used to access personal data by system users
3. Both 1 and 2 above
4. Log each transfer of storage media containing personal data to the computer facility

QUESTIONS 5-67 THROUGH 5-71 ARE TO BE JUDGED TRUE OR FALSE.

5-67. A suggested data processing procedure is to use control numbers to account for personal data upon receipt only.

1. True
2. False

5-68. Another suggested data processing procedure is to take regularly scheduled inventories of tape storage media only.

1. True
2. False

5-69. Another suggested data processing procedure is to verity the accuracy of the personal data aquisition and entry methods employed.

1. True
2. False

5-70. A suggested programming procedure is to subject all programming development and modification to a double-check by the program writer.

1. True
2. False

5-71. Another suggested programming procedure is to inventory current programs which process or access personal data.

1. True
2. False

5-72. A designated individual should be given the authority to oversee which of the following activities?

1. The installation practices in the storage, use, and processing of personal data
2. The use of physical security measures, information management, and computer system access controls
3. The internal uses and external transfer of data
4. Each of the above

QUESTION 5-73 IS TO BE JUDGED TRUE OR FALSE.

5-73. Audit reports should be maintained for routine inspection and used to provide additional data for tracing compromises of confidentiality.

1. True
2. False

Assignment 6

Systems Analysis

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 4-1 through 4-28

Learning Objective: Describe the steps in a systems analysis procedure and define the terminology in systems analysis as it relates to the military ADP community.

6-1. The term "systems analysis" is used by individuals in which of the following career fields?

1. Engineering
2. Scientific
3. Data Processing
4. Each of the above

6-2. The term "analysis" is defined in which of the following Federal Information Processing Standards Publications?

1. FIPS PUB 1
2. FIPS PUB 7
3. FIPS PUB 11-1
4. FIPS PUB 31-2

6-3. Of the following factors, which prevents the formulation of exact rules and standards for systems analyses to follow?

1. The use of shipboard computers
2. The use of the COBOL language on shore-based computers
3. The variety of different data processing systems that the Navy maintains
4. The lack of air-conditioned spaces for a standard computer system

6-4. The main objective of a systems analysis is to learn enough about a problem to implement a/an

1. cost savings
2. solution
3. economic study
4. time schedule

6-5. The Navy DP analyst's major functions involve solving problems for a command's

1. present computer system
2. future computer system
3. operations department
4. programming department

Learning Objectives: Define ADP terms as they are used in the ADP community.

6-6. In which of the following areas should a systems analyst have extensive knowledge and background?

1. Operations
2. Programming
3. Data management
4. All of the above

6-7. In which of the following areas should a problem analyst have extensive knowledge and background?

1. Operations
2. ADP management
3. ADP-oriented terminology
4. All of the above

6-8. In which of the following areas should a data analyst have extensive knowledge and background?

1. Writing system utilities
2. Programming FORTRAN
3. Programming COBOL
4. All of the above

6-9. A programming analyst should have an extensive background in

1. programming COBOL only
2. programming FORTRAN only
3. programming COBOL and FORTRAN
4. operations

6-10. Which of the following analysts should be able to solve complex problems in hardware and software interfacing?

1. A design analyst
2. A programming analyst
3. A data analyst
4. Each of the above

6-11. Which of the following items gives detailed instructions on how an analysis is conducted?

1. A project request
2. A systems study plan
3. An analyst guide
4. An operations manual

6-12. A DP may become involved in systems design when developing which of the following areas?

1. Software for a parent computer
2. Hardware for a parent computer
3. Software and hardware for a new system
4. Each of the above

Learning Objective: Explain the basic working fundamentals of a systems analyst and state the knowledge requirements.

6-13. What is the minimum number of months experience required on a computer system to receive a DP 2751 NEC?

1. One
2. Six
3. Three
4. Twelve

QUESTION 6-14 IS TO BE JUDGED TRUE OR FALSE.

6-14. A voluminous amount of material has been written about systems analysis in the DP rate training manuals in the past.

1. True
2. False

6-15. In which of the following branches, at most ADP facilities, is a systems analyst assigned?

1. Systems analysis and design
2. Operations
3. Programming
4. Data management

6-16. A systems analyst can be compared to a/an

1. Operator
2. Handyman
3. Programmer
4. Scientist

6-17. Which of the following duties could be the normal responsibility of a systems analyst?

1. Analyze hardware interfaces
2. Prepare reports
3. Evaluate available terminology
4. Each of the above

6-18. Of the following resources, which should a systems analyst evaluate when a new computer system is being implemented?

1. Money
2. Machines
3. Personnel
4. All of the above

6-19. Of the following ADP personnel, which one is the interface between all branches of an ADP facility?

1. A programmer
2. An analyst
3. A data base manager
4. An operator

6-20. Of the following ADP personnel, which one deals least with the technical portions of an existing system?

1. An analyst
2. An operator
3. A programmer
4. A data base manager

QUESTION 6-21 IS TO BE JUDGED TRUE OR FALSE.

6-21. To receive a 2751 NEC, a DP is required to possess a college degree in computer science.

1. True
2. False

6-22. Six months experience in which of the following areas of work is LEAST necessary to becoming a successfully trained DP, NEC 2751, systems analyst?

1. Operations
2. Programming
3. Electronics
4. Flow charting

6-23. After a minimum of how many months of ADP experience is an individual granted an analyst 2751 NEC?

1. Five
2. Two
3. Three
4. Six

6-24. A systems analyst with a 2751 NEC, and possessing an extensive background in programming, should be assigned to a systems study team as a

1. problem analyst
2. programming analyst
3. data analyst
4. design analyst

QUESTIONS 6-25 AND 6-26 ARE TO BE JUDGED TRUE OR FALSE.

6-25. A DP can become a qualified systems analyst by completing this nonresident career course.

1. True
2. False

6-26. A systems analyst must be skilled in the art and science of ADP problem solving.

1. True
2. False

6-27. Next to experience, which of the following factors is MOST critical in a person becoming a successful systems analyst?

1. The ability to generate a systems study guide
2. Dealing and conversing with people successfully
3. Creating a systems study flow chart
4. The ability to design a new software/hardware system

Learning Objective: Specify the objectives and procedures for a systems analysis. Relate the problems that generate a systems analysis to the different solutions which solve them.

6-28. Which of the following factors must an analyst determine when a problem exists?

1. What is taking place
2. What should be taking place
3. What does the user want to take place
4. All of the above

6-29. Systems analysis involves which of the following procedures?

1. Collecting facts
2. Organizing facts
3. Evaluating facts
4. All of the above

6-30. After the cost of a redesigned system is considered, the organization's information system is improved only if it increases the overall

1. input
2. output
3. speed
4. storage

6-31. Which of the following situations would usually generate a systems analysis study?

1. The present system sustained a single disk unit head crash
2. A user has a software problem
3. A system operates 24 hours a day
4. Each of the above

QUESTIONS 6-32 AND 6-33 ARE TO BE JUDGED TRUE OR FALSE.

6-32. Most computer systems operate perfectly, never need changes, and new requirements never exist.

1. True
2. False

6-33. The system has not been developed which is perfect and cannot be improved.

1. True
2. False

6-34. How many phases are in a systems analysis study for a previously funded computer system?

1. Five
2. Six
3. Seven
4. Eight

6-35. During which of the following phases is the systems analysis study team appointed?

1. Preparation phase
2. Interview/survey phase
3. Analysis/decision phase
4. Design phase

6-36. During which of the following phases is the scope of the analysis designed?

1. Analysis/decision phase
2. Preparation phase
3. Design phase
4. Interview/survey phase

6-37. During which of the following phases is the systems analysis study plan prepared?

1. Interview/survey phase
2. Design phase
3. Analysis/decision phase
4. Preparation phase

FOR QUESTIONS 6-38 THROUGH 6-46, CHOOSE FROM COLUMN B THE SYSTEMS ANALYSIS PHASE WHICH IS DESCRIBED IN COLUMN A. THE RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

A. PHASE DESCRIPTION	B. SYSTEMS ANALYSIS PHASE
6-38. Additional equipment is selected	1. Interview/survey phase
6-39. New programs are tested	2. Analysis/decision phase
6-40. The data end files involved in the analysis are determined	3. Design phase
6-41. All facts pertaining to the analysis study are collected	4. Implementation phase
6-42. The collected facts are analyzed	
6-43. Interviews are conducted	
6-44. If the results of an analysis are negative, a recommendation is submitted to upper management NOT to implement the analysis request	
6-45. New software/hardware modifications are designated	
6-46. Tests of the new system are performed and evaluated	

Learning Objective: Determine the working requirements of an analysis study team. Explain the different analysis phases and each step in a complete systems analysis.

6-47. Which of the following conditions will determine the number of members appointed to the study team?

1. The documentation required
2. The overall workload involved
3. The type of analyst required
4. The type of analysis required

6-48. A total systems analysis is conducted in accordance with what SECNAVINST series?

1. 5210.131
2. 5220.10
3. 5233.1
4. 5238.1

6-49. For a small systems addition, a minimum of how many analysts are usually assigned to conduct the study?

1. Five
2. Two
3. Three
4. Four

6-50. The first phase of a systems analysis study is the

1. interview/survey phase
2. preparation phase
3. analysis/decision phase
4. design phase

6-51. Of the following minimum totals, how many basic steps are in phase 1?

1. 10
2. 15
3. 20
4. 25

6-52. In which of the following steps of phase 1 is the study team appointed?

1. Step 5
2. Step 2
3. Step 7
4. Step 9

6-53. In which, if any, of the following steps of phase 1 is the scope of the analysis defined?

1. Step 5
2. Step 2
3. Step 3
4. None of the above

6-54. In which of the following steps of phase 1 is the analysis study team indoctrinated?

1. Step 5
2. Step 2
3. Step 6
4. Step 8

6-55. In which of the following steps of phase 1 are personnel interview schedules coordinated?

1. Step 9
2. Step 2
3. Step 3
4. Step 10

QUESTION 6-56 IS TO BE JUDGED TRUE OR FALSE.

6-56. The person in charge of the analysis should view the 10 steps of phase 7 as unchangeable.

1. True
2. False

6-57. When there is a problem on an existing funded system, the systems analysis study is approved by

1. the Chief of Naval Operations
2. the local command authority
3. higher authority
4. the Chief of Naval Personnel

6-58. If inexperienced analysts are assigned to the analysis branch, what minimum total of analysts should be appointed to each analysis project?

1. Five
2. Two
3. Three
4. Four

6-59. Members are usually assigned to the systems analysis study team by the

1. commanding officer
2. executive officer
3. OIC systems analysis branch
4. petty officer in charge, systems analysis branch

6-60. The scope statement of the analysis study should identify which of the following elements?

1. The operation
2. The system or subsystem
3. The areas affected
4. Each of the above

6-61. The scope of the analysis study should answer or identify which of the following problems?

1. The nature and purpose of the work products desired
2. The status of the system or subsystem (new or old)
3. The data files involved
4. Each of the above

6-62. Of the following documents, which one gets the analysis off to a correct start?

1. The operations manual
2. SECNAVINST 5231.1 series
3. The scope statement
4. The documentation manual

6-63. The fourth step of preparation (phase 1) is

1. the setting of time schedules
2. the setting of time clocks
3. the preparation of the scope statement
4. the briefing of personnel on schedules

6-64. How should the material be prepared for the analysis study plan?

1. As a loose leaf binder
2. As a bound document
3. Inserted in plastic covers
4. Sprayed with plastic paint

6-65. Which of the following items should always be included in a systems analysis study plan?

1. The written authority to conduct the analysis study
2. A written statement of the mission of the analysis study
3. A schedule showing when each major step is to be accomplished
4. All of the above

6-66. In which of the following situations should individuals be interviewed with questionnaires?

1. When the interviewee has a speech problem
2. When the interviewee takes annual leave
3. When it is inconvenient to interview the individual in person
4. When the interviewer is busy

6-67. Prior to an interview, which of the following data should be provided on an interview form?

1. Interviewee's name
2. Phone number of interviewee
3. Project number
4. All of the above

6-68. The remarks section of an interview form should contain a list of

1. individuals to be interviewed
2. appropriate questions for the interview
3. manuals to be utilized in the interview
4. phone numbers for the analysis study team numbers

6-69. During the eighth step of preparation (phase 1) the analysis team should be briefed on

1. the time element of the analysis
2. the cost of the analysis
3. all aspects of the analysis
4. the importance of coming to work on time

QUESTION 6-70 IS TO BE JUDGED TRUE OR FALSE.

6-70. All team member's questions should be answered during the briefing given in step 8 of preparation (phase 1).

1. True
2. False

6-71. Which of the following procedures should be accomplished in preparation (phase 1) step 9?

1. Interview schedules should be confirmed
2. The analysis team should be completed
3. The questionnaires should be completed
4. Data files should be checked for duplication

6-72. If time permits during preparation (phase 1) step 10, which of the following procedures is/are recommended prior to commencing detailed factfinding and interviewing?

1. A few days leave to relax
2. An orientation trip to the branches concerned with the analysis
3. A rewrite of all concerned documentation manuals
4. All of the above

Assignment 7

Interviews, Decision Making, and Data Base Management

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 4-29 through 5-8

Learning Objective: Recognize the procedures and practices used to conduct personnel interviews. Recognize the problems involved with interviewing and the different procedures available to conduct the interview correctly.

7-1. The main purpose of the interview/survey phase is to

1. gather opinions
2. gather facts
3. waste time
4. review hardware

7-2. Basically, facts are gathered using which of the following procedures?

1. Use existing documentation and survey the problem
2. Interview individuals in their environment
3. Document and collect data
4. All of the above

7-3. Which of the following procedures is/are accomplished in step 1 of the interview/survey (phase 2)?

1. Ensure that documentation manuals are current and determine that all procedures are being followed
2. Ensure that the analysis team is not over tasked
3. Ensure that operators follow orders
4. Ensure that programmers follow orders

7-4. What is the most powerful fact-finding tool available to the systems analyst?

1. Correct documentation
2. Personal interview
3. Questionnaire
4. Software

7-5. Who should control a systems analysis interview?

1. The systems analyst (interviewer)
2. The interviewee
3. A bystander
4. The commanding officer

7-6. An interview should be conducted by the analyst in the office of the

1. project manager
2. analyst
3. commanding officer
4. interviewee

QUESTION 7-7 IS TO BE JUDGED TRUE OR FALSE.

7-7. When conducting an interview, the systems analyst should be apologetic for interrupting the interviewee's work schedule.

1. True
2. False

7-8. Of the following practices, which one should be followed during an interview to eliminate the need for the analyst to return after the interview to verify facts?

1. Listen carefully during the interview
2. Be assisted by another analyst to help remember the facts
3. Take notes during the interview
4. Document the conversation the next day

7-9. Which of the following techniques should a systems analyst consider during an interview?

1. Do not make disparaging statements
2. Be a good listener
3. Ask frank and forthright questions
4. All of the above

QUESTIONS 7-10 THROUGH 7-17 ARE TO BE JUDGED TRUE OR FALSE.

7-10. Few individuals are nervous during interviews.

1. True
2. False

7-11. Some individuals have a tendency to supply answers that they feel are most favorable to the analyst, rather than give facts as they exist during an interview.

1. True
2. False

7-12. Some interviewee's will give information without actually checking their facts.

1. True
2. False

7-13. A cautious person never withholds valuable information during an interview.

1. True
2. False

7-14. A resentful individual is perhaps the most difficult source from which to get any type of information.

1. True
2. False

7-15. An analyst should NOT use tact when interviewing a resentful person.

1. True
2. False

7-16. The tone of the interview is a reflection of the physical and mental attitudes of the interested parties.

1. True
2. False

7-17. A systems analyst should express an opinion about the problem that is under analysis to the interviewee.

1. True
2. False

7-18. An interview should be limited to which of the following activities?

1. Information gathering
2. Fact gathering
3. Both 1 and 2 above
4. Opinions

7-19. What is the maximum time for an interview at one setting?

1. One hour
2. Two hours
3. Three hours
4. Four hours

7-20. If an interview is scheduled for an entire day, what is the minimum break time that should be scheduled every hour?

1. Five minutes
2. Six minutes
3. Nine minutes
4. Ten minutes

7-21. After an interview, which of the following items should be made using the information gathered?

1. Notes
2. A flowchart
3. A software program
4. A manual

7-22. After the interview, a copy of the interview should be returned for verification, corrections, and additions to which of the following individuals?

1. The systems analyst
2. The commanding officer
3. The department head
4. The interviewee

7-23. Information about a document or source data should be recorded on which of the following media as the information becomes available to the systems analyst?

1. A worksheet
2. A paper tape
3. A magnetic tape
4. A punched card

7-24. A worksheet should contain which of the following entries?

1. Opinions
2. Actual facts
3. Both 1 and 2 above
4. Estimates

Learning Objective: Recognize the different types of data and list various ways to assemble information for decision making. Recognize the proper way to sequence data and determine the correct manner in which to deal with large volumes of data collected in the first 2 phases of the analysis.

7-25. Which of the following is/are the primary purpose(s) of the analysis/decision phase?

1. To analyze bits and pieces of data
2. To draw conclusions about the data
3. To make recommendations to upper management
4. All of the above

7-26. The analysis/decision (phase 3) is divided into a minimum of how many steps?

1. One
2. Two
3. Three
4. Four

7-27. What procedure is performed in the first step of the analysis/decision (phase 3)?

1. Collect documents
2. Sequence documents
3. Interview individuals
4. Draw conclusions

7-28. Collected documents and data for an analysis can be sequenced into a mininum of how many categories?

1. One
2. Two
3. Three
4. Four

7-29. During which step of the analysis/decision (phase 3) is each document and piece of data information studied?

1. Step 1
2. Step 2
3. Step 3
4. Step 4

7-30. When collected documents and data are to be analyzed, which of the following items should be studied first?

1. Input to the system
2. Output of the system
3. Data in the system
4. Documents for the system

7-31. An understanding of which of the following items enables the analysis team to determine how information and data are transmitted into and out of the system?

1. Programming
2. Operations
3. System communications
4. System data files

7-32. An analysis of material pertaining to processing and storage usually results in areas where which of the following duplications is/are found?

1. Duplication of effort
2. Duplication of data elements
3. Duplication of reports
4. All of the above

7-33. What is the actual purpose of a system?

1. Productive output
2. Input
3. Data storage
4. Documentation

7-34. What statement dictates the type of locally prepared questions which should be asked about collected material?

1. The reason for the analysis
2. The scope of the analysis
3. The authority of the analysis
4. The type of analysis

7-35. Locally prepared questions about the material to be analyzed should produce information upon which to base

1. answers
2. questions
3. decisions
4. conclusions

7-36. An analysis study team should base their conclusions on

1. opinions
2. facts
3. directions from higher authority
4. directions from the user

7-37. In the analysis/decision phase (phase 3), the fourth step is for the systems analysis team to

1. be reassigned to their regular duties
2. make a written report to the official who authorized the study
3. collect any documents or data that are relevant to the study
4. interview the official who authorized the study

7-38. In the analysis/decision phase (phase 3), which of the following items should be contained in the report to upper management?

1. Specific recommendations for redesigning hardware configuration or software systems
2. Concise statements of anticipated benefits as a result of enacting the project request
3. A brief description of each modification to the present system
4. All of the above

7-39. If a project request is disapproved for implementation, a copy of which, if any, of the following items should be sent to the user by upper management?

1. The project request
2. The systems analysis study team's recommendation report
3. The letter assigning the systems analysis team
4. None of the above

7-40. Which of the following personal factors does a systems analyst utilize to solve the problem that generated the systems analysis?

1. Post experience
2. Ingenuity
3. Knowledge of ADP
4. All of the above

7-41. In what SECNAVINST series is the Mission Element Need Statement (MENS) explained?

1. 5230.1
2. 5231.1
3. 5510.1
4. 5510.131

QUESTION 7-42 IS TO BE JUDGED TRUE OR FALSE.

7-42. A paramount consideration in maintaining an optimum system is to avoid duplication.

1. True
2. False

7-43. The design phase 4 of a systems analysis consists of what total number of steps?

1. Five
2. Six
3. Seven
4. Four

7-44. The design or redesign of systems starts with the design or redesign of the systems

1. outputs
2. inputs
3. documentation
4. configuration

7-45. When a new system is designed, a requirement for which of the following items is generated?

1. New disk pack(s)
2. New tape drive(s)
3. New documentation
4. New data element library(ies)

7-46. At most commands, the systems analyst branch will be responsible for which of the following documentation manuals?

1. Data Requirement Document (RD)
2. Program Specification (PS)
3. Data Base Specification (DS)
4. All of the above

7-47. Different output media and media type should be taken into careful consideration by which of the following individuals?

1. The user
2. The systems analyst
3. Both 1 and 2 above
4. The tape librarian

7-48. To produce the desired output, it is essential that a new software system have accurate

1. input
2. documentation
3. card readers
4. terminals

7-49. Good input design and output results can be judged only by the

1. tape librarian
2. analyst
3. user
4. commanding officer

7-50. The first design consideration for any type of data base is the validation of

1. input data
2. output data
3. cost factors
4. documentation

7-51. How well the system functions and the quality of output both depend on the quality and dependability of the

1. hardware
2. data base
3. software
4. documentation

7-52. During which of the following steps in the design phase does the systems analyst actually design the programs necessary to produce the users request?

1. Step 1
2. Step 2
3. Step 3
4. Step 4

QUESTION 7-53 IS TO BE JUDGED TRUE OR FALSE.

7-53. The systems analyst performs the actual technical functions of programming and detailed data flow charting.

1. True
2. False

7-54. At the completion of step 4 of the design phase, the systems analyst should deliver the entire systems study plan to the

1. ADP department head
2. user
3. programming branch
4. operations officer

7-55. During the implementation phase, which of the following branches is responsible for the additional coordination between the user and other branches?

1. The users branch
2. The systems branch
3. The programming branch
4. The operations branch

7-56. For the technical development of any system, which of the following publications should be followed?

1. SECNAVINST 5231.1
2. FIPS publications
3. Local command policy
4. All of the above

7-57. During which of the following steps of the implementation phase should all testing be accomplished?

1. Step 1
2. Step 2
3. Step 3
4. Step 4

7-58. During the testing stages of the implementation phase, which of the following requirements should be completed?

1. All operations
2. All programming
3. All documentation
4. All of the above

QUESTION 7-59 IS TO BE JUDGED TRUE OR FALSE.

7-59. At the end of any systems study, the systems analyst can look back and see where improvements and different procedures could have been used in the study.

1. True
2. False

Learning Objective: Recognize the difference between data management systems and data base management systems, and define the terminology used within the ADP community when referring to data bases.

7-60. Which of the following improvements is/are claimed by manufacturers with each new software/hardware innovation developed?

1. Better endurance
2. Increased flexibility and speed
3. Longer durability
4. Increased ease and simplicity

7-61. Disciplined data control is embodied in a set of management procedures which is characterized as

1. data base management systems
2. data base organization
3. data base administration
4. data management systems

7-62. Which of the following terms is defined as any representation such as characters, to which meaning is or might be assigned?

1. Record
2. File
3. Byte
4. Data

7-63. Which of the following terms is defined as a set of data, part or the whole of another set of data, consisting of at least one file, that is sufficient for a given purpose or for a given data processing system?

1. Data base
2. Data link
3. Data collection
4. Data base management systems

7-64. Which of the following is characterized as a generalized software tool.

1. A data base
2. A Data Base Management System
3. Data logging
4. A data medium device

7-65. A software tool used to list all of the data elements in a data base is a

1. Data Catalog
2. Data Element Directory
3. Data Element Dictionary
4. data medium device

7-66. The software tool used to tell "what" and describe each data element in the data base is a

1. utility program
2. source program
3. Data Element Dictionary
4. Data Element Directory

7-67. Which of the following software tools is used to tell "where" each data element's location is in a data base?

1. Data Element Dictionary
2. Data Catalog
3. Data Description Language
4. Data Element Directory

7-68. The recording of data about events that occur in time sequence is known as

1. data striping
2. data logging
3. data storing
4. data recording

7-69. Which of the following characters or group of characters is used to identify an item of data?

1. A file number
2. A record address
3. A data name
4. A data library

7-70. Which of the following is an address which designates the storage location of an item of data to be treated as an operand?

1. Index
2. Absolute
3. Indirect
4. Direct

7-71. A set of related records treated as a unit is the definition of a

1. buffer
2. file
3. block
4. data base

7-72. Which of the following is a file in which the sequence has been reversed?

1. Sequential
2. Random
3. Variable
4. Inverted

7-73. What term is used to designate collection of related files?

1. A library
2. A data base
3. A master tape
4. An index

7-74. Which of the following abbreviations is a related example of a pushdown list?

1. LIFO
2. FIFO
3. GIGO

7-75. An ordered set of items of data is termed a/an

1. organization
2. list
3. chart
4. print

Assignment 8

Data Base Software Tools and the WWMCCS Operations Community

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 5-10 through 6-7

Learning Objective: Describe the duties of the individual who creates, manages, and manipulates data base software tools.

8-1. In an ADP facility that has a data base branch within the organizational structure, the DP performs the function of

1. librarian
2. data base administrator
3. disk pack custodian
4. analyst supervisor

8-2. Which of the following is one of the main goals of data base administration?

1. To create data programs to calculate numbers
2. To reduce the duties and functions of an analyst
3. To optimize usage of data in a shared data base environment
4. To aid managers in technical knowledge of the system

8-3. A key requirement for effective data base administration is having a/an

1. software system that never faults
2. third generation computer system
3. analyst that diagnoses only data
4. technically competent DP staff

QUESTIONS 8-4 AND 8-5 ARE TO BE JUDGED TRUE OR FALSE.

8-4. A data base can be better managed if each programmer controls and maintains his/her own data base and files.

1. True
2. False

8-5. Better controlled and more up-to-date data can result in increased responsiveness to the various user communities.

1. True
2. False

8-6. Which of the following indications signify(ies) the need for data base administration?

1. Proliferating data bases
2. Overlapping requirements
3. Lack of data integrity
4. All of the above

8-7. What is the minimum pay grade recommended before a DP should be appointed as a DBA?

1. DP3
2. DP2
3. DP1
4. DPC

8-8. All _____(a)_____ requests or (unusual), (usual) violations of command policy concerning the data base should be coordinated with _____(b)_____ (middle), (upper) management.

1. (a) unusual (b) middle
2. (a) unusual (b) upper
3. (a) usual (b) middle
4. (a) usual (b) upper

8-9. What minimum number of basic qualifications should an individual possess before being appointed as a command's DBA?

1. Five
2. Two
3. Three
4. Six

8-10. A DBA should possess what minimum number of months operations experience on the system to which assigned?

1. Five
2. Six
3. Three
4. Four

8-11. A DBA should possess what minimum number of months programming experience on the system to which assigned?

1. Six
2. Seven
3. Three
4. Four

8-12. A DBA should have a thorough knowledge of which of the following SECNAV instructions?

1. 5200.18 (Series)
2. 5200.20 (Series)
3. 5233.1 (Series)
4. All of the above

QUESTION 8-13 IS TO BE JUDGED TRUE OR FALSE.

8-13. The DP DBA's organizational role is usually characterized as administrative only.

1. True
2. False

8-14. Usually, a minimum of how many DPs are charged with the responsibility for coordinating, controlling, and directing activities in a data base environment?

1. One
2. Two
3. Three
4. Four

8-15. The definition of data elements and data relationships should be based on which, if any, of the following needs?

1. On a clear understanding of each participating user community's requirement
2. On the programming language most often used by the programming staff
3. On the type of recording media determined to be necessary by the operations branch
4. None of the above

8-16. Which, if any, of the following languages should be utilized to define and structure a data base?

1. COBOL
2. PASCAL
3. FORTRAN or BASIC
4. None of the above

QUESTION 8-17 IS TO BE JUDGED TRUE OR FALSE.

8-17. The DBA should not be involved with the procurement of new hardware pertinent to the data base.

1. True
2. False

8-18. A data base security function is intended to guard against unauthorized access to the

1. ADP facility
2. computer room
3. data base
4. tape library

8-19. Of the following individuals, which one(s) should be responsible for the continued well-being of the data base enviornment?

1. The operations supervisor
2. The tape librarian
3. The DBA
4. All of the above

Learning Objective: Explain the difference between DBMS and DMS, and explain the functions of software tools utilized in a DBMS.

8-20. A DBMS is a software system that is intended to manage and maintain data in a (a) (redundant), (nonredundant) structure for the purpose of being processed by (b) (single), (multiple) applications.

1. (a) redundant (b) single
2. (a) redundant (b) multiple
3. (a) nonredundant (b) single
4. (a) nonredundant (b) multiple

8-21. A DBMS retains relationships between different data elements within the

1. CPU
2. tape controllers
3. data base
4. ADP facility

8-22. A DMS is intended primarily to permit access to which of the following areas?

1. Tape libraries
2. Already existing files
3. CPU O/S macro modules
4. Offline utilities

8-23. The principle intent of a DMS is to perform which of the following functions?

1. Report generation
2. Single application inquiry
3. Information retrieval
4. All of the above

8-24. DED/D systems are different from DBMS in that their main thrust is to provide control over which of the following resources within an organization?

1. Hardware
2. Data
3. Personnel
4. All of the above

8-25. In early designs of ADPS, data seldom crossed organizational boundaries. This situation resulted in (a) (single), (multiple) definitions of the same data as (b) (independent), (dependent) data files were generated creating data redundancy.

1. (a) single (b) dependent
2. (a) multiple (b) independent
3. (a) single (b) independent
4. (a) multiple (b) dependent

8-26. The advent of DBMS helped solve many information problems by organizing

1. data elements
2. software tools
3. ADP shops
4. personnel

QUESTIONS 8-27 AND 8-28 ARE TO BE JUDGED TRUE OR FALSE.

8-27. The DBMS has fully integrated all data resources within the Navy.

1. True
2. False

8-28. The benefits realized from the DED/D are directly related to the effective collection, specification, and management of the total data resources of an organization.

1. True
2. False

8-29. Which, if any, of the following is a deciding factor when determining the name for a data base software package?

1. The complications involved when controlling the usage of the package
2. The amount and type of information the package provides the user
3. The amount of core storage the package utilizes in the CPU
4. None of the above

8-30. Most of the commercially available data base software packages are of which of the following types?

1. Data Element Dictionaries
2. Data Element Directories
3. Data Element Catalogs
4. Data Element Dictionary/ Directory

8-31. A DED/D provides the means for defining and describing which, if any, of the following elements of a data base?

1. Contents
2. Characteristics
3. Capacity
4. None of the above

8-32. The basic intent of DED/D's security features is to control the access to

1. the data elements
2. the CPU
3. time sharing
4. the computer room

8-33. Usually, who has the highest level of security control in a DED/D?

1. The operations officer
2. The data base administrator
3. The ADP department head
4. The systems analyst

8-34. After a DED/D's dictionary/ directory function has been grouped as a primary or secondary, it can be subdivided, according to their implementation, into which of the following categories?

1. Distinctive
2. Freestanding
3. Dependent
4. Both 2 and 3 above

QUESTION 8-35 IS TO BE JUDGED TRUE OR FALSE.

8-35. A primary DED/D is always part of another system, such as a DBMS.

1. True
2. False

8-36. A subdivision, freestanding or dependent DED/D, differs from a primary DED/D's function only in

1. theory
2. implementation
3. installation
4. performance

8-37. In the civilian market, freestanding DED/Ds are known as

1. specific DED/Ds
2. generalized DED/Ds
3. perfect DED/Ds
4. DBMS-DED/Ds

8-38. Which of the following software systems does a dependent DED/D support?

1. Independent utilities
2. Compilers
3. DBMS
4. All of the above

8-39. When interfaces are used between DBMS and DED/Ds, which of the following abilities is/are provided to the user?

1. The ability to define the data base to the DED/D
2. The ability to generate data element definitions for a DBMS from an up-to-date DED/D
3. The ability to exercise control over the data elements of a DBMS using DED/D facilities
4. All of the above

8-40. A secondary DED/D is an integral physical part of another system and functions as a(n)

1. software and hardware interface
2. data and file predefinition mechanism
3. data transmitting software buffer
4. arithmetic subroutine to the operating software

8-41. The _____(a)_____ DED/D (primary), (secondary) has more security control over data elements and has _____(b)_____ (extensive), _____ reporting and retrieval (modest) capabilities.

1. (a) primary (b) extensive
2. (a) secondary (b) modest
3. (a) secondary (b) extensive
4. (a) primary (b) modest

8-42. A major advantage of utilizing a DED/D is that it helps the data base administrator control and maintain the data resources of an organization.

1. True
2. False

Learning Objective: Explain the purpose and functions of DBMS, SCHEMA, and SUB-SCHEMAS.

8-43. Which of the following features of a DBMS is the most important?

1. Easy access to the data
2. The storage and maintenance of large volumes of data
3. The capability for sharing the data resources

QUESTIONS 8-44 THROUGH 8-48 ARE TO BE JUDGED TRUE OR FALSE.

8-44. The DBMS has solved all of data base software problems.

1. True
2. False

8-45. In a DBMS environment users do not want to share their data with other users of the data base.

1. True
2. False

8-46. Technical and nontechnical DBMS users have different views of data.

1. True
2. False

8-47. A conventional computer system has many application programs or systems using different data bases and files.

1. True
2. False

8-48. On a conventional computer system, a lesser chance of error exists when updating all the common data in different data bases than would exist if a DBMS was used.

1. True
2. False

8-49. Which, if any, of the following statements best describes a DBMS schema?

1. It is the actual data in the data base framework
2. It is the software description of the operating system
3. It is the overall logical data base description or framework
4. None of the above

8-50. Which of the following items enhance security factors and help prohibit data compromise?

1. A subroutine
2. A data converter
3. A cryotron
4. A subschema

8-51. Which, if any, of the following is a description of a data item?

1. An occurrence of a bit in a data base
2. An occurrence of the largest unit of named data
3. An occurrence of the smallest unit of named data
4. None of the above

8-52. A data aggregate is an occurrence of a named collection of data items within a

1. file
2. system
3. record
4. byte

8-53. A vector is a _____(a)_____ (one-dimensional), _____ sequence of (two-dimensional) data items, all of which have _____(b)_____ (different), (identical) characteristics.

1. (a) one-dimensional
   (b) different
2. (a) two-dimensional
   (b) different
3. (a) one-dimensional
   (b) identical
4. (a) two-dimensional
   (b) identical

8-54. Which of the following is a unique value which identifies a record in the data base to a run unit?

1. An actual key
2. A data base key
3. A search key
4. A sort key

8-55. An occurrence of a named collection of records is called a

1. key
2. keyword
3. set
4. mark

8-56. Each set occurrence must contain what minimum number of occurrences of its defined owner type of record?

1. One
2. Two
3. Three
4. Four

8-57. A named collection of records which need NOT preserve owner/member relationships is called a/an

1. Set
2. Area
3. Data base key
4. Data item

8-58. In a DBMS environment, conceptually, what is the User Working Area (UWA)?

1. A shop working area for users
2. An area provided for object programs
3. A loading and unloading zone where data is placed
4. A subroutine building area

8-59. After the data base physical description has been examined, which, if any, of the following items keys the actual physical record to be read?

1. DBMS
2. The object program
3. The console operator
4. None of the above

8-60. When data has been requested by a DBMS, to which of the following areas does the operating system deliver the requested data from the data base?

1. User Work Area (UWA)
2. System buffer area
3. DBMS
4. All of the above

8-61. After the operating system has transferred data to the system buffer area, where does the DBMS deliver the data to be utilized by a source program?

1. A system work disk
2. A system work tape
3. The User Work Area (UWA)
4. System buffer area 1 and 2

8-62. Which of the following items are contained in a Data Description Language (DDL)?

1. Reserved words
2. Key words
3. Literals
4. All of the above

QUESTIONS 8-63 THROUGH 8-66 ARE TO BE JUDGED TRUE OR FALSE.

8-63. There may be data types defined in the subschema which have characteristics and representations different from those of any schema type.

1. True
2. False

8-64. The implementor may provide special conversion procedures in addition to those provided in DBMS for implementing conversion rules.

1. True
2. False

8-65. The relationship between a DDL and a DML is the relationship between definitions and the host language.

1. True
2. False

8-66. A storage schema describes the representation of stored data in device independent terms.

1. True
2. False

Learning Objective: Describe the different command structures associated with the WWMCCS operations community.

8-67. The WWMCCS community is supported by what computer system?

1. UNIVAC 1500 system
2. IBM 360/50 system
3. Honeywell 6000 system
4. UNIVAC 1100 system

8-68. Elements of the WWMCCS are maintained to ensure maximum responsiveness to which of the following organizations?

1. National Command Authorities
2. Joint Chiefs of Staff
3. Fleet Commanders
4. Unified Commands

8-69. The NCA consists of which of the following individuals?

1. Unified commanders
2. The President
3. The Secretary of Defense
4. Both 2 and 3 above

8-70. What organization is the priority component of the WWMCCS?

1. NAVDAC
2. NMCS
3. NARDAC
4. NAVSEA

8-71. Which of the following DOD Directive series provides policy guidance and establishes responsibilities for the management of WWMCCS?

1. 4730.1
2. 5100.30
3. 5510.1
4. 5510.131

8-72. The effective operation and support of the WWMCCS within the Navy requires that it be recognized as which of the following types of systems?

1. Symbolic
2. Monostable
3. Nonintegrated
4. Integrated

QUESTIONS 8-73 AND 8-74 ARE TO BE JUDGED TRUE OR FALSE.

8-73. The Navy's WWMCCS community is supported only by a single Honeywell 6060 processor configuration.

1. True
2. False

8-74. The Navy's WWMCCS community Honeywell 6000 systems are standard and NEVER vary in size.

1. True
2. False

8-75. Which of the following OPNAVINST series sets forth software/hardware applications, operation requirements, and complete management procedures of the WWMCCS new standard computer system?

1. 5110.4
2. 5200.16
3. 5230.12
4. 5400.1

Assignment 9

WWMCCS Honeywell Computer

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 6-8 through 6-48

Learning Objective: Describe the operations of the General Comprehensive Operating Supervisor in the WWMCCS Honeywell Computer.

9-1. In which of the following modes does the Honeywell 6000 operate?

1. Single-processing
2. Multiprogramming
3. Multiprocessing
4. Both 2 and 3 above

9-2. The series 6000 Honeywell computer was designed and built for maximum

1. downtime
2. uptime
3. maintenance
4. deallocation

9-3. What software maintains the status of all peripherals, memory, processors, and user jobs in the system?

1. DMAP
2. PMAP
3. XREF
4. GCOS

9-4. The allocator queue accommodates a number of jobs by using the system

1. ports
2. scheduler
3. monitor
4. multiplexor

9-5. GCOS allocates system resources to jobs in the allocator queue in accordance with the priority of the

1. queue
2. system
3. job
4. programmer

9-6. GCOS can supervise the concurrent execution of a maximum of how many programs?

1. Twenty-one
2. Forty-three
3. Sixty-three
4. Seventy-two

9-7. How are catalogs and files secured on the Honeywell 6000 computer?

1. By an armed guard
2. By passwords and permissions
3. By a time sharing software package
4. By a wired source program

9-8. Concurrent remote processing capabilities can be added to the Honeywell 6000 by including which of the following types of hardware?

1. Remote batch processing card readers
2. Dual channel disk
3. Front-end network processors
4. Multiplex channel processors

9-9. Which of the following language capabilities is/are on the Honeywell 6000?

1. ABACUS
2. ALGOL
3. FORTRAN
4. All of the above

QUESTIONS 9-10 THROUGH 9-13 ARE TO BE JUDGED TRUE OR FALSE.

9-10. Batch mode programs can be initiated from time sharing terminals.

1. True
2. False

9-11. The series 6000 Document Entry Subsystem (DS 6000) is a hardware system only.

1. True
2. False

9-12. The message switch system stores messages in a journal before forwarding it to the addressed destination.

1. True
2. False

9-13. The message switching dimensions control is entirely within the Honeywell 6000 CPU.

1. True
2. False

9-14. The Total Online Testing System is composed of what minimum number of subsystems?

1. Five
2. Two
3. Three
4. Four

9-15. What maximum number of concurrent diagnostic programs can operate with user programs under the GCOS?

1. Six
2. Seven
3. Eight
4. Twelve

Learning Objective: Identify the hardware characteristics of the WWMCCS Honeywell Computer.

9-16. Which of the following system modules provide the required amount of directly addressable primary memory?

1. Bulk Store Subsystem Modules
2. Memory Modules
3. Processor Modules
4. Input/Output Modules

9-17. Which of the following system modules controls data communication functions and provide services to remote users?

1. Input/Output Modules
2. Data Entry Controller Modules
3. Front-End Network Processor Modules
4. Processor Modules

9-18. The Honeywell 6000 GCOS operating system automatically adapts itself to control any

1. Honeywell 6000 equipment configuration
2. manufacturer's equipment configuration
3. software packages
4. logic circuit boards

9-19. Every processor and IOM connects to each memory module through

1. channels
2. ports
3. conduit
4. plug boards

9-20. Each memory module is composed of a

1. CPU
2. system controller
3. associated memory units
4. system controller and associated memory units

9-21. The memory module serves the processor by acting as a

1. program executor
2. arithmetic calculator
3. logic manipulator
4. passive system component

9-22. Each access in the memory module is composed of 2 parity lists and what maximum number of 9-bit bytes?

1. Eight
2. Ten
3. Twelve
4. Four

9-23. The Honeywell 6000 series memory is organized into what maximum number of word blocks?

1. 256
2. 1024
3. 4096
4. 9999

9-24. The memory's system controller has what maximum number of parts for connection to active modules?

1. Six
2. Seven
3. Eight
4. Four

9-25. Which of the following benefits is achieved by operating the memory module on a 72-bit parallel basis?

1. Less tape wear
2. More system usage of software
3. Increased system throughput
4. Less power consumption

9-26. The processor's operation unit performs which of the following operations?

1. Arithmetic
2. Instruction fetching
3. Address preparation
4. All of the above

9-27. The processor's control unit performs which of the following operations?

1. Arithmetic
2. Logic
3. Data storing
4. All of the above

9-28. The processor has what maximum number of different modes of operation?

1. One
2. Two
3. Three
4. Four

QUESTIONS 9-29 THROUGH 9-32 ARE TO BE JUDGED TRUE OR FALSE.

9-29. When the processor is in master mode, GCOS allows unrestricted access to all of memory.

1. True
2. False

9-30. When the processor is in slave mode, user programs cannot be executed.

1. True
2. False

9-31. When the processor is in slave mode, program execution is limited by a time register.

1. True
2. False

9-32. The Base Address Register (BAR) is used for memory protection functions in the master mode.

1. True
2. False

9-33. Which of the following registers contains the absolute address of a users program?

1. The timer register
2. The BAR register
3. The A register
4. The Q register

9-34. The timer register is used by the GCOS to time programs for which of the following transactions?

1. Input quantity
2. Output quantity
3. Automatic termination
4. Priority change

9-35. What minimum number of special processing status conditions, termed "faults," is on the Honeywell 6000 computer?

1. Eight
2. Sixteen
3. Thirty-two
4. Sixty-four

9-36. Peripheral device operations are controlled by processor prepared control word lists stored in which of the following areas of memory?

1. Arithmetic region
2. Control region
3. Middle region
4. Communications region

9-37. The communications region of memory is referred to as

1. GCOS
2. Slave area
3. IOM mailboxes
4. Master area

9-38. Each IOM Module provides direct access to what pieces of hardware?

1. Disk controllers
2. Tape drives
3. Each memory module
4. Unit Record Controllers

9-39. The IOM multiplexer is the coordinator of which of the following system operations?

1. Tape movement
2. Input/Output
3. Disk control
4. Printer speed

9-40. What maximum number of I/O subsystems can be controlled per IOM?

1. Fourteen
2. Twenty-four
3. Thirty-four
4. Forty-four

9-41. Each IOM can transfer what maximum number of characters per second?

1. Six hundred
2. Six thousand
3. Six million
4. Six billion

Learning Objective: Describe the remote input/output operations of the WWMCCS Honeywell Computer.

QUESTIONS 9-42 AND 9-43 ARE TO BE JUDGED TRUE OR FALSE.

9-42. Output time is reduced on the Honeywell 6000 through the use of multiple local and remote input/output devices.

1. True
2. False

9-43. The DATANET 355 FNP has a memory size of 16,384 words only.

1. True
2. False

9-44. The DATANET 355 FNP has a minimum cycle time of how many microseconds?

1. One
2. Two
3. Three
4. Four

9-45. What maximum number of adapters on the DATANET 355 FNP will accommodate a total data transfer rate of 500,000 words per second?

1. Eight
2. Sixteen
3. Thirty-two
4. Four

9-46. The DATANET 355 is a storage-oriented computer with which of the following hardware modules included?

1. Independent memory
2. Processor
3. Input/Output
4. All of the above

9-47. The DATANET 355 FNP can handle what maximum number of teleprinter users?

1. 100
2. 200
3. 300
4. 400

9-48. The DATANET 355 FNP can handle what maximum number of CRT subsystems?

1. Eight
2. Sixteen
3. Thirty-two
4. Sixty-four

9-49. The multiline communications controller HSLA can utilize what maximum number of concurrently operating lines?

1. 32
2. 64
3. 128
4. 256

9-50. The HSLA channels can be configured in any combination NOT to exceed what maximum number of terminals total per HSLA?

1. Eight
2. Sixteen
3. Thirty-two
4. Sixty-four

9-51. What maximum number of terminals can be connected to the DATANET 355 FNP through the LSLA at 110 bps?

1. Sixteen
2. Thirty-two
3. Fifty-two
4. Sixty-four

Learning Objective: Identify the 6000 Series characteristics of the WWMCCS Honeywell Computer.

9-52. Which of the following series 6000 model computers have the Extended Instruction Set (EIS) processors?

1. The 6040
2. The 6060
3. The 6080
4. All of the above

9-53. All active 6000 series modules connect to all system controllers and have common access to

1. printers
2. slave systems
3. tape libraries
4. memory

9-54. What maximum number of standard interfaces is available on the IOM for the connection of peripheral controls?

1. One
2. Two
3. Three
4. Four

9-55. The primary function of a control console is to provide for direct communications between the operator and the

1. GCOS
2. IOM
3. DATANET 355 FNP
4. DATA bank

9-56. The master console connects to a common peripheral interface channel of the

1. DATANET 355 FNP
2. slave computer
3. IOM
4. printer

9-57. The console accepts input data via which of the following hardware devices?

1. A channel
2. A keyboard
3. A magnetic tape
4. A disk

9-58. On the DSS181B disk, data is grouped in what total number of continuously addressable sectors?

1. 72
2. 720
3. 7,200
4. 72,000

9-59. On the DSS181B disk, what maximum number of sectors is accessible in each cylinder?

1. 36
2. 360
3. 3,600
4. 36,000

9-60. On the DSS181B disk there are $\frac{\text{(a)}}{(18),\ (20)}$ sectors per track and $\frac{\text{(b)}}{(18),\ (20)}$ tracks per cylinder.

1. (a) 18 (b) 18
2. (a) 20 (b) 20
3. (a) 18 (b) 20
4. (a) 20 (b) 18

9-61. On the DSS181B disk subsystem a maximum dual-channel crossbar with 32 disk-pack drives provides a capacity of what maximum number of characters?

1. 589 thousand
2. 884 thousand
3. 589 million
4. 884 million

9-62. A DSS181B disk subsystem's basic configuration can be expanded up to a 221 million character capacity by adding what minimum number of additional disk-pack drives?

1. Five
2. Two
3. Three
4. Four

9-63. On the MTH500 magnetic tape handler, the average rewind speed is

1. 500 ips
2. 200 ips
3. 300 ips
4. 400 ips

9-64. Which of the following tape densities is/are provided on the MTH500?

1. 556 BPI
2. 800 BPI
3. 1,600 BPI
4. All of the above

9-65. A single-channel magnetic tape subsystem connected to an IOM permits reading or writing of any one of what maximum number of magnetic tape units connected to that control?

1. Six
2. Eight
3. Twelve
4. Four

9-66. What maximum number of unit record devices can be controlled simultaneously by a unit record control?

1. Six
2. Seven
3. Eight
4. Four

9-67. The CRZ301 card reader can read what maximum number of cards per minute?

1. 150
2. 500
3. 1,000
4. 1,050

9-68. The PRT303 train printer can print what maximum number of lines per minute?

1. 600
2. 800
3. 1,100
4. 1,150

9-69. The PRT303 has which, if any, of the following features?

1. Photo-cell print train
2. Power-driven hood
3. Swing-out paper folders
4. None of the above

9-70. The PRT303 can print an original and what maximum number of copies?

1. Five
2. Two
3. Three
4. Four

9-71. The standard print trains for the PRT303 are the BCD set with $\frac{\text{(a)}}{(63), (94)}$ printable characters and the ASCII set (upper/lower case) with $\frac{\text{(b)}}{(63), (94)}$ printable characters?

1. (a) 63 (b) 63
2. (a) 94 (b) 94
3. (a) 94 (b) 63
4. (a) 63 (b) 94

9-72. The PRT303 printer skips paper at what maximum number of inches per second?

1. Fifty
2. Sixty
3. Seventy
4. Eighty

9-73. The CRZ301 card reader uses which, if any, of the following types of card input devices?

1. Vacuum advance
2. Photoelectric
3. Manual feed
4. None of the above

9-74. The CRZ301 card reader has a maximum stacker capacity of how many cards?

1. 1,000
2. 2,000
3. 2,500
4. 4,000

Assignment 10

Documentation

Textbook Assignment: DP TECH 1 & C, NAVEDTRA 10265-D; pages 7-1 through 7-38

Learning Objective: Recognize the definition of documentation as it relates to ADP in the Navy and SECNAVINST 5233.1 (Series).

10-1. A document is any record that can be described by which of the following characteristics?

1. Has permanence
2. Can be read by a human
3. Can be read by a machine
4. Each of the above

10-2. ADP documentation preparation standards are discussed in what SECNAV instruction series?

1. 5230.6
2. 5231.1
3. 5233.1
4. 5252.5

10-3. ADP documentation standards are discussed in what Department of Defense (DOD) instruction?

1. 5200.8
2. 5228.1
3. 7935.1
4. 10462.1

10-4. Upon adoption of ADP in the Navy, which of the following methods of passing information became less desirable?

1. From person to document
2. From person to person
3. From document to person
4. From document to document

10-5. Which of the following is/are (a) purpose(s) of documentation?

1. To help managers determine if requirements have been met
2. To help managers determine if resources should continue to be expended
3. To record technical information
4. All of the above

IN QUESTIONS 10-6 THROUGH 10-9, SELECT THE DOCUMENT MNEMONIC FROM COLUMN B THAT IS ASSIGNED TO THE DOCUMENT LISTED IN COLUMN A. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. DOCUMENTS	B. MNEMONIC
10-6.	System/Subsystem Specification	1. FD
10-7.	Data Requirements Documents	2. SS
10-8.	Program Specifications	3. RD
10-9.	Functional Descriptions	4. PS

10-10. Which of the following documents can include three manuals and be bound as one document?

1. Users Manual
2. Project Manuals
3. Program Specifications
4. Functional Descriptions

10-11. What is the maximum number of pages that should be utilized in a project manual?

1. 199
2. 201
3. 299
4. 301

10-12. Which of the following manuals are combined to create a project manual?

1. Users, Computer Operations, and Functional Description
2. Computer Operations, Data Requirements Documents, and Users
3. Computer Operations, Users, and Program Maintenance
4. Users, Program Maintenance, and Data Base Specifications

10-13. A commanding officer may authorize minimum documentation requirements in a Users Manual under which of the following circumstances?

1. When programs have no identifiable use elsewhere in the government
2. When only E-6 personnel are assigned to the command
3. When the computer mainframe has remote terminals attached
4. When only civilians are assigned to the programming staff

10-14. An annotated program listing should be included in the

1. Computer Operations Manual
2. Users Manual
3. Test Plan
4. Test Analysis Report

IN QUESTIONS 10-15 THROUGH 10-18, SELECT THE DOCUMENT MNEMONIC FROM COLUMN B THAT IS ASSIGNED TO THE DOCUMENT LISTED IN COLUMN A. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. DOCUMENTS	B. MNEMONIC
10-15.	Computer Operations Manual	1. MM
10-16.	Program Maintenance Manual	2. PT
10-17.	Test Plan	3. RT
10-18.	Test Analysis Reports	4. OM

10-19. A document that reports the results of a developmental study is a

1. Technical Report
2. Technical Note
3. Test Plan
4. Test Analysis Report

10-20. A document that provides procedures and other information that does NOT logically belong in other types of documents is a

1. Technical Report
2. Technical Note
3. Test Plan
4. Test Analysis Report

Learning Objective: Recognize in general the different components of each documentation manual.

10-21. Of the following statements, which one is correct concerning the Computer Operation Manual (OM)?

1. The manual sets forth standards for tape libraries
2. The manual is a self-standing document when all informational requirements are met
3. The manual is designed to initiate a data base
4. The manual never contains precise or detailed information

IN QUESTIONS 10-22 THROUGH 10-28, SELECT FROM COLUMN B THE COMPONENT'S STATUS (MANDATORY, AS REQUIRED, OR OPTIONAL) IN THE MANUAL FOR EACH COMPONENT LISTED IN COLUMN A. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. COMPONENTS	B. COMPONENT STATUS
10-22.	Table of contents	1. Mandatory
10-23.	Record of changes	2. As required
10-24.	Appendices	3. Optional
10-25.	Index	
10-26.	Front cover	
10-27.	Special notices	
10-28.	Back cover	

Learning Objective: Discuss, in brief, the information required on the front cover of a document.

10-29. The document title and subtitle on the front cover of a document may include which of the following items?

1. The author's name
2. A page count
3. The activity's short name
4. A superseding statement

10-30. Of the following items, which one(s) make(s) up the document number?

1. A control number
2. A project number
3. Both 1 and 2 above
4. A stock number

IN QUESTIONS 10-31 THROUGH 10-34, SELECT FROM COLUMN B THE CHARACTER POSITION NUMBER OF THE PROJECT NUMBER THAT UNIQUELY IDENTIFIES THE FUNCTIONAL PURPOSE OF EACH CHARACTER LISTED IN COLUMN A. RESPONSES IN COLUMN B MAY BE USED MORE THAN ONCE.

	A. FUNCTIONAL PURPOSES OF EACH CHARACTER OF THE PROJECT NUMBER	B. THE PROJECT NUMBER CHARACTER POSITION
10-31.	The character(s) that specify(ies) the function of the project	1. First and second character
10-32.	The character(s) that identify(ies) organization responsible for development of the project	2. Third character 3. Fourth character 4. Fifth, sixth, and seventh characters
10-33.	The character(s) that indicate(s) the requesting organization	
10-34.	The character(s) that form(s) a serial number	

10-35. Of the following control number characters, which one designates the classification of the document?

1. The first
2. The second
3. The third
4. The fourth

10-36. Of the following characters, which one(s) designate(s) the document type count in the control number?

1. The first
2. The second and third
3. The fourth and fifth
4. The sixth

10-37. Which, if any, of the following types of characters is used to identify a document that has been revised?

1. An alphabetic
2. A numeric
3. A special character
4. None of the above

10-38. On what basis is the title page prepared for each document?

1. Optional
2. Mandatory
3. On an "as required" basis

10-39. On what basis are special notice components prepared for a document?

1. Mandatory
2. As required
3. Optional

10-40. Of the following items, which one(s) is/are contained in a special notice component?

1. Information concerning the status of the document
2. Letters of promulgation
3. Instructions for the documents' handling
4. All of the above

10-41. An abstract component is mandatory in which of the following documents?

1. DS
2. PM
3. PS
4. SS

10-42. An abstract component does NOT exceed _____ (250 words), (250 sentences), is preferably _____ (classified), (unclassified), and summarizes the function, scope, purpose, and content matter described in the document.

1. (a) 250 words (b) classified
2. (a) 250 sentences (b) classified
3. (a) 250 words (b) unclassified
4. (a) 250 sentences (b) unclassified

10-43. Of the following language forms, which one should NOT be included in an abstract component?

1. Abbreviations
2. Complete sentences
3. Narrative paragraphs
4. Special characters

10-44. On what basis are table of contents components prepared for a document?

1. Optional
2. As required
3. Mandatory

10-45. If a document is NOT expected to have frequent changes, when should a record of change component be inserted?

1. When the document is printed
2. When the document is canceled
3. When the document has figures
4. When the document has its first change

10-46. When classified pages are to be added within a change transmittal notice, which of the following document components is mandatory as part of the change?

1. A new index
2. A new abstract
3. A new list of figures
4. A new list of effective pages

10-47. The instructions, content requirement, and format for which of the following documents should be reviewed prior to taking advancement in rate examinations?

1. UM
2. OM
3. MM
4. Each of the above

10-48. On what basis are appendices prepared for a document?

1. Mandatory
2. As required
3. Optional

10-49. Which, if any, of the following appendices provides definitions for acronyms used within a document?

1. Bibliography
2. References
3. Terms and Abbreviations
4. None of the above

10-50. A reference appendix is provided in a document when more than what minimum number of sources is cited in the text?

1. One
2. Five
3. Seven
4. Ten

10-51. How should references be listed in the reference appendix?

1. In numerical order
2. In alphabetical order
3. In command hierarchy
4. In the order referenced in the text

10-52. How should indirect reference sources be listed in the bibliography appendix?

1. In alphabetical order by the author's last name
2. In alphabetical order by the author's first name
3. In alphabetical order by the source's title
4. In chronological order by the source's publishing date

10-53. On what basis is an index component prepared for a document?

1. Mandatory
2. As required
3. Optional

10-54. On what basis is a distribution component prepared for a document?

1. Mandatory
2. As required
3. Optional

10-55. On what basis is a back-cover component prepared for a document?

1. Mandatory
2. As required
3. Optional

10-56. Of the following elements, which one may be required on the back-cover component of a document?

1. The command's name
2. The page number
3. The activity's seal
4. The security classification if the component is classified

Learning Objective: Discuss, in general, document documentation requirements and determining factors for documenting requirements at various ADP installations.

10-57. Of the following individuals, which one is a main factor in determining the number of documents to be provided for a project?

1. The operations division officer
2. The tape librarian
3. The operations CPO
4. The ultimate user

10-58. When should a maximum amount of documentation be provided for a project?

1. Only when the IBM 03/360 system is used
2. When the project is small
3. When the project is simple
4. When the project is large and complex

10-59. In figure 7-8 of the text, what is the maximum number of complexity factors assigned to each factor column?

1. One
2. Five
3. Three
4. Four

10-60. In figure 7-8, if there were two (2) check marks in column one, three (3) check marks in column two, and five (5) check marks in column four, what would be the total project's complexity value?

1. Seven
2. Ten
3. Twenty-one
4. Twenty-eight

10-61. At most commands, the function of establishing minimum documentation requirements is delegated to the

1. user
2. systems analyst
3. head programmer
4. project manager

Learning Objective: Recognize the distinctive characteristics of each document type and function.

10-62. The FD (Functional Description) document should be written in which of the following types of language?

1. COBOL
2. Computer-oriented
3. FORTRAN
4. Noncomputer-oriented

10-63. The term "data element" refers to a data element or its use in a data system and is often called the

1. data user identification
2. data use identifier
3. data system use
4. data manipulator

10-64. Which of the following documents may be written after the preparation of an SS (System/Subsystem Specification) document to expand on the SS document requirements?

1. A UM
2. An OM
3. A PS
4. An FD

10-65. For which of the following individuals is a DS (Data Base Specification) document prepared?

1. Programmers
2. Analysts
3. Operators
4. Users

10-66. In some instances, a UM is the only document required for a computer program. Of the following components, which one must also be provided with a UM (Users Manual)?

1. A program flowchart
2. An annotated program source listing
3. A formal explanation statement
4. A systems study outline

10-67. Of the following documents, which one contains detailed information necessary to initiate, run, and terminate a particular system?

1. The PT
2. The FD
3. The OM
4. The RT

10-68. Of the following documents, which one provides a presentation of the computer program system test deficiencies for review by management?

1. The PT
2. The RT
3. The PS
4. The SS

Learning Objective: Identify all aspects of project development.

10-69. During which of the following phases of an ADS development life cycle is a project request prepared?

1. During the initiation phase
2. During the development phase
3. During the evaluation phase
4. During the operation phase

10-70. Of the following items, which one may be included in a project request?

1. Points of contact for additional data
2. Desired milestone dates
3. Environmental constraints
4. Each of the above

10-71. During the development phase, which of the following stages is included?

1. Design
2. Integration
3. Installation
4. Each of the above

10-72. During what stage of an ADS development life cycle is it determined if contractors are to be utilized?

1. Initiation
2. Definition
3. Design
4. Programming

10-73. During what phase or stage is a Functional Description (FD) document prepared?

1. Definition
2. Design
3. Programming
4. Evaluation

10-74. During what phase or stage is a Program Specification (PS) document prepared?

1. Definition
2. Design
3. Programming
4. Evaluation

10-75. During what phase or stage is a Computer Operation Manual prepared?

1. Definition
2. Design
3. Programming
4. Evaluation

☆U.S. GOVERNMENT PRINTING OFFICE: 1981 — 740-086/24

COURSE DISENROLLMENT

All study materials must be returned. On disenrolling, fill out only the upper part of this page and attach it to the inside front cover of the textbook for this course. Mail your study materials to the Naval Education and Training Program Development Center.

PRINT CLEARLY

NAVEDTRA NUMBER	COURSE TITLE
10265-D	Data Processing Technician 1 & C

Name Last First Middle

Rank/Rate Designator Social Security Number

COURSE COMPLETION

Letters of satisfactory completion are issued only to personnel whose courses are administered by the Naval Education and Training Program Development Center. On completing the course, fill out the lower part of this page and enclose it with your last set of answer sheets. Be sure mailing addresses are complete. Mail to the Naval Education and Training Program Development Center.

PRINT CLEARLY

NAVEDTRA NUMBER	COURSE TITLE
10265-D	Data Processing Technician 1 & C

Name

ZIP CODE

MY SERVICE RECORD IS HELD BY:

Activity

Address ZIP CODE

Signature of enrollee

A FINAL QUESTION: What did you think of this course? Of the text material used with the course? Comments and recommendations received from enrollees have been a major source of course improvement. You and your command are urged to submit your constructive criticisms and your recommendations. This tear-out form letter is provided for your convenience. Typewrite if possible, but legible handwriting is acceptable.

Date _____

From: _____
(RANK, RATE, CIVILIAN)

_____

_____ ZIP CODE _____

To: Naval Education and Training Program Development Center (PD 6)
Pensacola, Florida 32509

Subj: RTM/NRCC Data Processing Technician 1 & C, NAVEDTRA 10265-D

1. The following comments are hereby submitted:

(Fold along dotted line and staple or tape)

(Fold along dotted line and staple or tape)

DEPARTMENT OF THE NAVY
NAVAL EDUCATION AND TRAINING PROGRAM
DEVELOPMENT CENTER (PD 6)
PENSACOLA, FLORIDA 32509

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
NAVY DEPARTMENT
DoD-316

NAVAL EDUCATION AND TRAINING PROGRAM DEVELOPMENT CENTER
BUILDING 2435 (PD 6)
PENSACOLA, FLORIDA 32509

PRINT OR TYPE

Data Processing Technician 1 & C
NAVEDTRA 10265-D

NAME _____ ADDRESS _____
Last First Middle Street/Ship/Unit/Division, etc.

City or FPO State Zip

RANK/RATE _____ SOC. SEC. NO. _____ DESIGNATOR _____ ASSIGNMENT NO. _____

☐ USN ☐ USNR ☐ ACTIVE ☐ INACTIVE OTHER (Specify) _____ DATE MAILED _____

SCORE

	1 (T)	2 (F)	3	4		1 (T)	2 (F)	3	4		1 (T)	2 (F)	3	4
1	☐	☐	☐	☐	26	☐	☐	☐	☐	51	☐	☐	☐	☐
2	☐	☐	☐	☐	27	☐	☐	☐	☐	52	☐	☐	☐	☐
3	☐	☐	☐	☐	28	☐	☐	☐	☐	53	☐	☐	☐	☐
4	☐	☐	☐	☐	29	☐	☐	☐	☐	54	☐	☐	☐	☐
5	☐	☐	☐	☐	30	☐	☐	☐	☐	55	☐	☐	☐	☐
6	☐	☐	☐	☐	31	☐	☐	☐	☐	56	☐	☐	☐	☐
7	☐	☐	☐	☐	32	☐	☐	☐	☐	57	☐	☐	☐	☐
8	☐	☐	☐	☐	33	☐	☐	☐	☐	58	☐	☐	☐	☐
9	☐	☐	☐	☐	34	☐	☐	☐	☐	59	☐	☐	☐	☐
10	☐	☐	☐	☐	35	☐	☐	☐	☐	60	☐	☐	☐	☐
11	☐	☐	☐	☐	36	☐	☐	☐	☐	61	☐	☐	☐	☐
12	☐	☐	☐	☐	37	☐	☐	☐	☐	62	☐	☐	☐	☐
13	☐	☐	☐	☐	38	☐	☐	☐	☐	63	☐	☐	☐	☐
14	☐	☐	☐	☐	39	☐	☐	☐	☐	64	☐	☐	☐	☐
15	☐	☐	☐	☐	40	☐	☐	☐	☐	65	☐	☐	☐	☐
16	☐	☐	☐	☐	41	☐	☐	☐	☐	66	☐	☐	☐	☐
17	☐	☐	☐	☐	42	☐	☐	☐	☐	67	☐	☐	☐	☐
18	☐	☐	☐	☐	43	☐	☐	☐	☐	68	☐	☐	☐	☐
19	☐	☐	☐	☐	44	☐	☐	☐	☐	69	☐	☐	☐	☐
20	☐	☐	☐	☐	45	☐	☐	☐	☐	70	☐	☐	☐	☐
21	☐	☐	☐	☐	46	☐	☐	☐	☐	71	☐	☐	☐	☐
22	☐	☐	☐	☐	47	☐	☐	☐	☐	72	☐	☐	☐	☐
23	☐	☐	☐	☐	48	☐	☐	☐	☐	73	☐	☐	☐	☐
24	☐	☐	☐	☐	49	☐	☐	☐	☐	74	☐	☐	☐	☐
25	☐	☐	☐	☐	50	☐	☐	☐	☐	75	☐	☐	☐	☐